ZKAccess 4.0 User Manual

Version: 1.1

Date: Nov. 2010

About This Manual

This document introduces the main function, the user interface and operations of the system. For installation, please refer to the Quick Installation Guide.

Table of Contents

1. System Instruction 1

1.1 Functions Instruction 1
1.2 Basic Operation Flow 2

2. System Management 4

3. My Work Panel 7

4. Personnel System Management 9

4.1 Department management 9
4.2 Personnel management 10
4.2.1 Add personnel 10
4.2.2 Personnel Information Maintenance 12
4.2.3 Personnel adjustment 14

5. Device Management 15

5.1 Area settings 15
5.2 Device management 16
5.2.1 Add access control panel 16
5.2.2 Device maintenance 19
5.3 Device Communication Management 20

6. Security System Management 22

6.1 Access control time zones 23
6.2 Access control holiday 24
6.3 Door settings 26
6.3.1 Door management 26
6.3.2 First-Card Normal Open 31
6.3.3 Multi-Card Opening 33
6.3.4 Interlock settings 35
6.3.5 Anti-passback settings 36
6.3.6 Linkage setting 37
6.4 Access levels 39
6.5 Personnel access levels 40
6.6 Real-time monitoring 41
6.7 Access control reports 45

7. System Settings 48

7.1 User management 48
7.2 Database management 50
7.3 System parameters 54
7.4 Log records 54

8. Appendices 55

Appendix 1 Common operation 55
Appendix 2 END-USER LICENSE AGREEMENT FOR THIS SOFTWARE 63
Appendix 3 FAQs 66

Definitions

Super user: The user who has all operation levels of the system, which can assign new users (such as company management personnel, registrar, access control administrator) in the system and configure the roles of corresponding users.

Role: During daily use, the super user needs to assign new users having different levels. To avoid individual setting for each user, roles having certain levels can be set in role management, and then be assigned to specified users.

Access Control Time Zone: It can be used for door timing. The reader can be made usable during valid time periods of certain doors and unusable during other time periods. Time zone can also be used to set Normal Open time periods of doors, or set access control levels so that specified users can only access specified doors during specified time periods (including access levels and First-Card Normal Open settings).

Door Status Delay: The duration for delayed detection of door sensor after the door is opened. Detection is performed only after the door is opened and the delay duration expired. When the door is not in the "Normally Open" period, and the door is opened, the device will start timing. It will trigger alarm when the delay duration expired, and stop alarm when you close the door. The door status delay should be longer than lock drive duration.

Close and Reverse-lock: Set locking or not after door closing.

Lock Drive Duration: Used to control the delay for unlocking after card punching.

First-Card Normal Open: During a specified interval, after the first card punching by a person having First-Card Normal Open level, the door will be Normal Open, and will automatically restore closing after the valid interval expired.

Multi-Card Opening: This function needs to be enabled in some special access occasions, where the door will open only after consecutive card punching by several people. Before verifying, any card punching out of this combination (even the card belong to other combination) will interrupt the procedure, and you need to wait 10 seconds to restart verifying. It will not open upon card punching by one of the combination.

Interlock: Can be set for any two or more lock belong to one access control panel, so that when one door is opened, the others will be closed. And you can open one door only when others are closed.

Anti-pass Back: The card holder who entered from a door by card punching must exit from the same door by card punching, with the entry and exit records strictly consistent.

Linkage Setting: When an event is triggered at an input point of the access control

system, a linkage action will occur at the specified output point to control such events as verification, opening, alarm and exception of the system and list them in the corresponding monitored report for view by the user.

1. System Instruction

1.1 Functions Instruction

The security management is increasing concerns of modern enterprises. This management system facilitates customers to integrate operation of safety on one platform, making access control management easier and more reasonable, so as to improve efficiency.

❁ System Features

1. Powerful data processing capacity, allowing management of the access control data of 30,000 people.

2. Visible and reasonable work flows come from abundant experience in access control management.

3. Automatic user name list management.

4. Multilevel management role-based level management secures user data confidentiality.

5. Real-time data acquisition system ensures prompt feedback of access control data to the management.

6. Support GPRS, WIFI and other wireless data transmission modes.

❁ Configuration requirements:

CPU: Master frequency of 2.0G or above;

Memory: 1G or above;

Hardware: Available space of 10G or above;

❁ Operating system:

Supported operation systems: Windows XP/ Windows 2003/ Windows Vista/ Windows 7

Supported databases: MySQL (system default)/ MS SQL Server/ Oracle

❁ System modules:

The system includes four major functional modules:

Personnel system: Primarily two parts: first, department management settings, used to set the Company's organizational chart; second, personnel management settings,

used to input personnel information, assign departments, maintain and manage personnel.

Device system: Set communication parameters for device connection, including system settings and machine settings. After successful communication, the information of connected devices can be viewed, and such operations as remote monitoring, uploading and downloading can be performed in the system.

Access control system: WEB-based management system, enabling normal access control functions, management of networked access control panel via computer, and unified personnel access management. The access control system sets door opening time and levels for registered users, so that some users are permitted to unlock some doors through verification during certain intervals.

System settings: Primarily used to assign system users and configure the roles of corresponding module; management database, such as backup, initialization and recovery; and set system parameters and manage system operation logs.

1.2 Basic Operation Flow

The following are the basic steps to use the system, based on the role of a super user. Different users have different operation levels, so the steps may slightly differ. The user just needs to follow the steps below and skip the items which is not displayed on your interface.

Step 1: Log in to the system to modify the default password of the account;

Step 2: Assign accounts and roles to system users (such as company management personnel, registrar, access control administrator);

Step 3: Set system parameters, database, notice, reminder and other frequently used system information;

Step 4: The user sets departmental organization chart refer to the organizational chart of your company;

Step 5: Input company personnel and conduct daily maintenance of the personnel;

Step 6: Set access control time zones and access control holidays (as access control exceptions);

Step 7: Add devices to the system, and configure the basic information of devices;

Step 8: Set parameters for access controlled doors;

Step 9: Set access levels to establish access control based on doors group and time zones;

Step 10: Set the access levels of personnel by assigning personnel to access levels to decide which people can open which doors during which time zones.

2. System Management

1. Log in to the system

After installing the server on the computer, the user can access the server through the network and use this system.

Open the browser and enter the server's IP address in the address bar. Press [Enter] to access the system homepage.

If you use the program at server computer, please open the [Server Controller] first, and start the service. Then double click the **[ZKAccess4.0 Security System]** shortcut on the desktop, the following homepage pops up.

Note: Please right click [Server Controller] and select [Run as Administrator] in Windows 7/Vista system.

Before accessing the system, for system security, it is required to verify identity. We will provide a super user (having all operation levels) for the beginner of this system. Enter user name and password, and click [login] to enter the main interface of the system.

Note: The user name of the super user is [admin], and the password is [admin]. After first login to the system, for system security, please use [Modify password] function to modify the password.

The super user can assign system users to company personnel (such as company management personnel, registrar, access control administrator) and configure the roles of corresponding modules. For details, see 7.1 User management.

2. Quit the system:

Click [Logout] button on the upper right corner of the interface to return to ZKAccess 4.0 homepage.

Or close the browser directly to quit the system.

After that, enter the [Server Controller] and stop the server, then quit the [Server Controller].

3. Customize settings:

The user can use this function to customize the main interface. Click [Setting] to activate the Setting interface, and enter the following information: E-mail address, First Name, Last Name, and Language. Click [Confirm] to complete setting.

The modified system interface will change accordingly, such as the desired language.

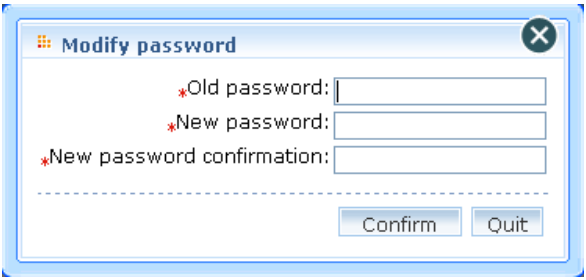
4. System user manual:

The system help file. On each operation interface, a "" icon will appear on the right top of the interface, indicating the help for the current page. Click it to view the help file.

5. Modify password:

The super user and the new user created by the super user (the default password for the new user is "111111") can use the [Modify password] function to modify the login password for system security. Click [Modify password] to pop up the edit Page. Enter the old password and the new password, confirm the new password and click

[Confirm] to complete the modification.



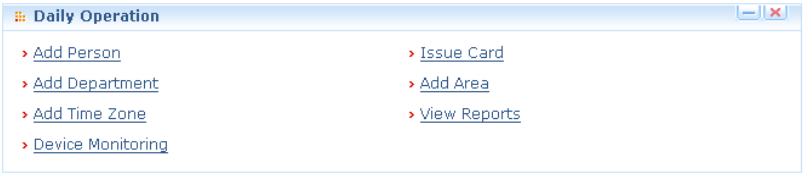
Note: The user name is case-insensitive, but the password is case-sensitive.

3. My Work Panel

After the user log in to the system, it will show the [My Panel] main interface, displaying common operation and other important information.

The default work panel includes the following modules:

❁ **Common operation:** The user can rapidly perform some common operation here, as shown below.



Add Person please refer to 4.2.1 Add personnel;

Card Issue please refer to 4.2.2 Personnel Information Maintenance;

Add Department please refer to 4.1 Department management;

Add Area please refer to 5.1 Area Settings;

Add Time Zone please refer to 6.1 Access control time period;

View Reports please refer to 6.7 Access control reports;

Device monitoring please refer to 5.3 Device Communication Management;

❁ **Access Control Quick Start:** Follow the steps to enter corresponding modules for related operation, thus basically fulfilling access control functions.

Access Control Quick Start
Step 1: Device Management
Step 2: Personnel Management
Step 3: Time Zone Settings
Step 4: Holidays Settings
Step 5: Door Configuration
Step 6: Create Access Levels
Step 7: Personnel Access Levels Settings
Step 8: Real-Time Monitoring

Device management please refer to 5.2 Device management;

Personnel management please refer to 4.2 Personnel management;

Time zone settings please refer to 6.1 Access control time zone;

Holidays settings please refer to 6.2 Access control holiday;

Door configuration please refer to 6.3 Door settings;

Create access levels please refer to 6.4 Access levels;

Personnel access levels settings please refer to 6.5 Personnel access levels settings;

Real-time monitoring please refer to 6.6 Real-time monitoring;

Customize Work Panel:

Click [Customize Work Panel] on the upper right corner to pop up a dialog box. Cancel the tick of your undesired modules (all ticked by default), and click [OK] to complete setting. Now customized modules are displayed;

Or directly click the " " icon on a module to minimize, and click " " to close the module. Click the upper bar to drag and adjust its position;

To restore the original panel, click [Restore Work Panel] to refresh and return to the system default work panel.

4. Personnel System Management

Before using the system's access control management functions, first access the personnel system for configure: First, department management settings, used to set the company's organizational chart; Second, personnel management settings, used to input personnel, assign departments, and maintain and manage personnel. Then set access control.

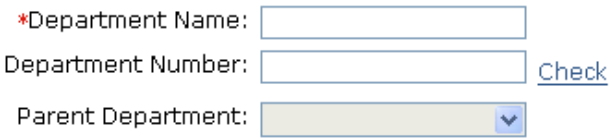
4.1 Department management

Before managing company personnel, it is required to describe and manage the departmental organization chart of the company. Upon first use of the system, by default it has a primary department named **[Company Name]** and numbered **[1]**. This department can be modified but can't be deleted.

Main functions of department management include add department and department maintenance.

1. Add Department:

Click [Personnel] - [Department] - [Add department] to show add department edit interface:



The fields are as follows:

Department name: Any character, up to a combination of 40 characters;

Department number: If required, it shall not be identical to another department. The length shall not exceed 5 digits. Click [Verify] to see if repeated or not;

Parent department: Select from the pull-down menu and click [OK];

After editing, click [OK] to complete adding, or click [Cancel] to cancel it.

To add a department, you can also use [Import] to import department information from other software or document into this system. For details, see Appendix 1 Common Operation. [Upper Department] is an important parameter to determine the Company's organizational chart. On the right of the interface, the Company's organizational chart will be shown in the form of department tree.

2. Department Maintenance:

Department maintenance includes department edit and delete:

Upon change of department or organizational structure, the user can use [Edit] function to modify such items as department name, department number or upper department. Click department name directly or click the [Edit] button behind the department to access edit interface for modification.

To delete a department, click the check box before the department, and click [Cancel Department], or directly click the [Delete] button behind the department.

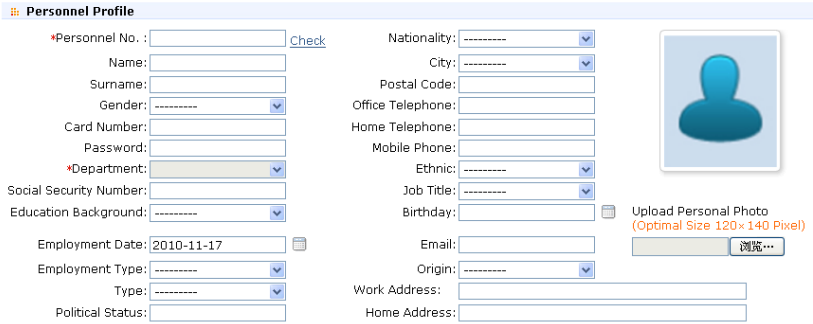
Note: A department can not be deleted freely. If so, the personnel under the department will be pending, and some historical data will be unable to be queried. If deletion is required, please first transfer the departmental personnel to other department.

4.2 Personnel management

When starting to use this management program, the user shall register personnel in the system, or import personnel information from other software or document into this system. For details, see Appendix 1 Common Operation.

4.2.1 Add personnel

Click [Personnel] - [Personnel] - [Add] to show personnel profile edit interface:



The fields are as follows:

Personnel No.: By default, the length shall not exceed 9 digits. A number with a length of less than 9 digits will be preceded with 0 automatically to complete 9 digits. Numbers can not be repeated. Click [Verify] to see if it is repeated or not;

Department: Select from the pull-down menu and click [OK]. If the department was not set previously, you can only select the default [Company Name] department;

Social Security Number: Repetition is not allowed. Click [Verify] to check repetition. 15-digit and 18-digit ID card numbers are supported;

Card Number: Assign a card number to the person for access control use. This can be done manually or by using card issuer. For details, see personnel card issue in 4.2.2 Personnel Maintenance;

Password: Set personnel password. An access control panel only supports 6-digit passwords. If a password exceeds the specified length, the system will truncate it automatically;

Personal Photo: The best size is 120×140 pixels, for saving space. For details, see upload personal photo in 4.2.2 Personnel Maintenance;

Employment Date: By default it is the current date.

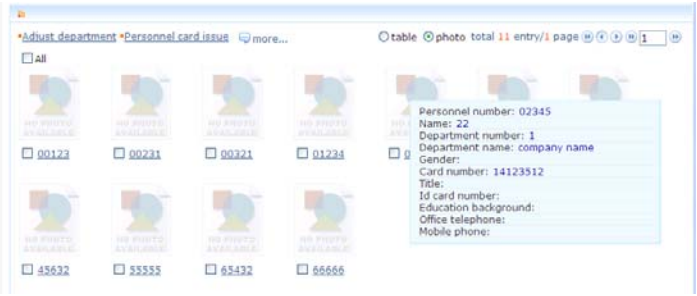
Access Control Settings: Select access levels, start and end dates of access validity time, multi-card opening personnel groups (Presetting is required. For details, see 6.3.3 Multi-Card Opening);

Validity time are set for temporary access control, where the door can be opened only during this time period. If not ticked, the setting will be always valid.

After editing personnel information, click [OK] to save and quit, and added personnel will be shown in the personnel list.

Note: The number of a person, whether departed or in service, must be unique. The system, when verifying, will automatically search the number in the departure library.

The personnel information list, by default, is displayed as a table. If graphic display is selected, photos and numbers will be shown. Put the cursor on a photo, the particulars about the personnel will be shown.



4.2.2 Personnel Information Maintenance

Includes such operations as Personnel Card Issue and Upload Personal Photo.

For such functions, you can directly click the personnel number in the personnel list to enter the edit interface for modification, or click [Edit] button under "Related operation" to enter the edit interface for modification. After modification, click [OK] to save and quit.

1. Personnel card issue:

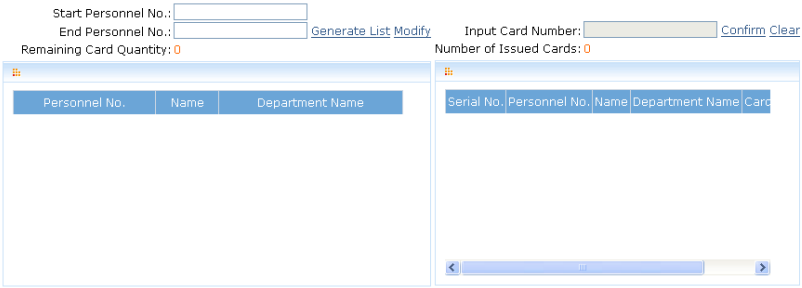
Assign card numbers to personnel, including batch card issue and individual card issue.

(1) How to use the card issuer:

The card issuer is connected to the PC through USB port. When the cursor is on the card number input box, punch the card on the card issuer, then the card number will display in the input box.

(2) Batch card issue:

Click [Personnel] - [Card issue] - [Batch card issue] to show the batch card issue edit interface;



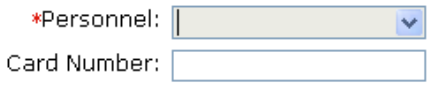
Enter start and end personnel numbers (not longer than the system support max digits) to generate personnel list and show this all personnel without cards within this number interval;

Enter card number (or use card issuer for card issue). Each time clicking [OK], card numbers will be assigned to personnel in the list, until all personnel are provided with cards;

Click [OK] to complete card issue and return. Personnel and corresponding card numbers will be shown in the list.

(3) Individual card issue:

Click [Personnel] - [Card issue] - [Add] to show individual card issue interface;

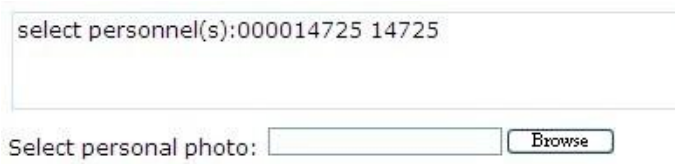


Select personnel, enter card number (or use card issuer for card issue), select card issue date, and click [OK].

Note: A person can be issued cards for many times, and the last card issue will prevail. The system supports card issue through card issuer and by manually inputting card numbers.

2.. Upload personal photo:

Click [Personnel] - [Personnel], tick the personnel (only one person can be selected), click [Upload personal photo], enter the edit interface, click [browse] and select a photo, and click [OK] to save and exit.



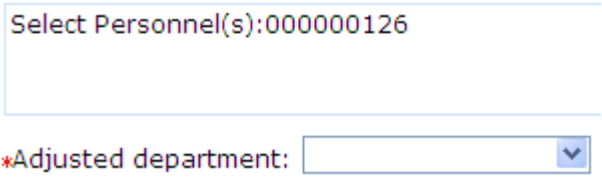
4.2.3 Personnel adjustment

Personnel adjustment is daily maintenance of existing personnel, primarily including: personnel adjust department and delete personnel.

1. Personnel adjust department:

Operation steps are as follows:

(1) Click [Personnel] - [Personnel], and select the person subject to department adjustment from the personnel list, click [Adjust Department] button, the following interface appear:



(2) Select the department to be transferred to

(3) After editing, click [OK] to save and quit.

2.. Delete personnel:

Click [Personnel] - [Personnel], select personnel, click [Delete], and click [OK] to delete, or directly click [Delete] under "Related operation" of the personnel to delete.

Note: Deleting personnel also results in deleting the personnel in database.

5. Device Management

Access control panel to be connected to this system provides access control system functions. To use these functions, the user must first install devices and connect them to the network. Second, set corresponding parameters in the system so as to manage these devices via the system, upload user access control data, download configuration information, output reports and achieve digital management of the enterprise.

Device management primarily includes area setting, device management, and device monitoring.

5.1 Area settings

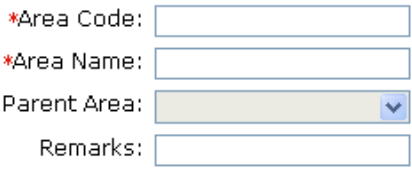
Area is a spatial concept, facilitating the user to manage devices in a specific area.

In the access system, after area setting, devices (doors) can be filtered by area upon real-time monitoring.

The system, by default, has set an area named [Headquarters] and numbered [1]. Area settings include add area and delete area.

1. Add area:

Click [Device] - [Area settings] - [Add] to activate the add area edit interface:



The fields are as follows:

Area Number: Repetition not allowed;

Area Name: Any character, up to a combination of 30 characters;

Parent Area: Decides the regional organization structure of the company.

After setting, click [OK].

2. Delete area:

Select area, click [Delete area], or directly click [Delete area] under “Related

operation" of an area, and click [OK].

5.2 Device management

Set the communication parameters of connected devices. Only when communication parameters, including system settings and device settings, are correct, normal communication with devices will be possible. When communication is successful, you can view the information of connected devices, and perform remote monitoring, uploading and downloading data.

To add access control panel, search and view devices connected to the network, and directly add from the searching result.

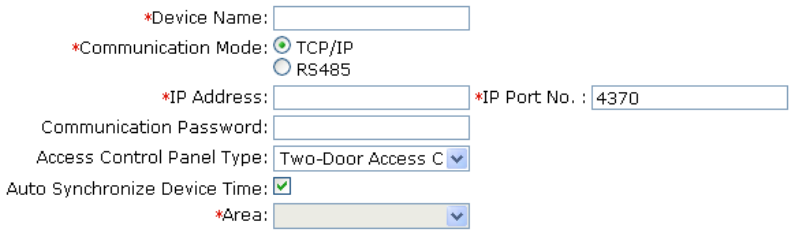
5.2.1 Add access control panel

There are two way to add access control panel.

1. Add device:

(1) Click [Device] - [Device] - [Add] to show the device information edit interface. The communication modes are TCP/ IP or RS485. The following interface will be shown:

TCP/ IP:



IP address: Please enter the IP address of the access control panel;

IP port No.: In Ethernet mode, the default is 4370;

RS485:

Serial port number: COM1-COM254;

485 address: The machine number. When serial port numbers are the same, there will be no repeated 485 addresses;

Baud rate: Same as the baud rate of the device (9600/ 19200/ 38400/ 57600/115200). The default is 38400;

Device name: Any character, up to a combination of 20 characters;

Communication password: Any character, up to a combination of 16 characters. You need to input this field only when you add a new device with the communication password. It can't be modify when you edit the device information except in [Modify communication password] operation. Please refer to 6.3.1 Door management.

Note: You need not input this field if the device has no communication password, such as it is new factory device or just after the initialization.

Panel type: One-door panel, two-door panel, four-door panel;

Switch to two-door two-way: When four-door panel is selected, this box will appear. By default, it is not ticked. This parameter is used to switch the four-door one-way access control panel to two-door two-way access control panel (For changes of extended device parameters before and after switching, see relevant files of access control panel).

Note: After the four door one-way access control panel is switched to two-door two-way access control panel, to switch back, you need delete the device from the system and add it again. When adding, do not tick the check box before this parameter.

Auto synchronize device time: By default it is ticked, namely, it will synchronize device time with server time each time connecting the device. If it is not ticked, the user can manually synchronize device time;

Area: Specify areas of devices. After area setting, devices (doors) can be filtered by area upon real-time monitoring.

(2) After editing, click [OK], and the system will try connecting the current device:

If connection is successful, it will read corresponding extended parameters of the device. At this time, if the access control panel type selected by the user does not meet the corresponding parameters of the actual device, the system remind the user. If the user clicks [OK]to save, it will save the actual access control panel type of the device;

Extended device parameters: Serial number, device type, firmware version number, auxiliary input quantity, auxiliary output quantity, door quantity, and reader quantity.

If device connection fails, while the user still needs to add the device to the system, corresponding device parameters and extended parameters, such as serial number, will not be written into the system, and such settings as anti-passback and linkage will be impossible. These settings can be created only when the device is reconnected successfully and corresponding parameters are acquired.

Access control panel settings:

❁ TCP/ IP communication requirements:

Support and enable TCP/ IP communication, directly connect the device with PC or connect to the Internet, get the device IP address and other information of the device;

❁ RS485 communication requirements:

Support and enable RS485 communication, connect to PC through RS485, get the serial port number, RS485 machine number (address), baud rate and other information of the device.

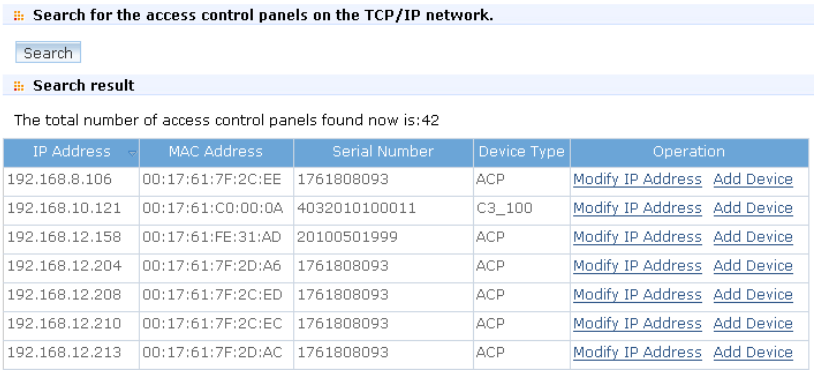
2. Add device by searching access control panels:

Search the access control panels in the Ethernet.

(1) Click [Device] - [Device] - [Search panels], to show the search interface;

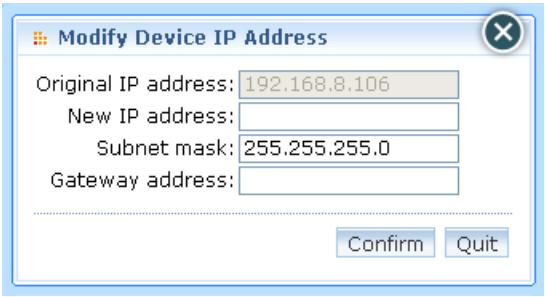
(2) Click [Start search], and it will prompt [searching……];

(3) After searching, the list and total number of access control panels will be displayed;


Search for the access control panels on the TCP/IP network.
Search
Search result
The total number of access control panels found now is:42
IP Address
MAC Address
Serial Number
Device Type
Operation
192.168.8.106 00:17:61:7F:2C:EE 1761808093 ACP Modify IP Address Add Device
192.168.10.121 00:17:61:C0:00:0A 4032010100011 C3_100 Modify IP Address Add Device
192.168.12.158 00:17:61:FE:31:AD 20100501999 ACP Modify IP Address Add Device
192.168.12.204 00:17:61:7F:2D:A6 1761808093 ACP Modify IP Address Add Device
192.168.12.208 00:17:61:7F:2C:ED 1761808093 ACP Modify IP Address Add Device
192.168.12.210 00:17:61:7F:2C:EC 1761808093 ACP Modify IP Address Add Device
192.168.12.213 00:17:61:7F:2D:AC 1761808093 ACP Modify IP Address Add Device

(4) Click [Add to device list] behind the device, and the browser may pop up a security tip. Right-click to select [Window temporarily allowing script execution], click [Add to device list] behind the device again, and a dialog box will pop up. Enter self-defined device name, and click [OK] to complete device adding.

(5) The default IP address of the access control panel may conflict with the IP of a device on the Internet. You can modify its IP address: Click [Modify IP address] behind the device, and a dialog box will pop up. Enter the new IP address and other parameters(gateway and subnet mask are not necessary);



5.2.2 Device maintenance

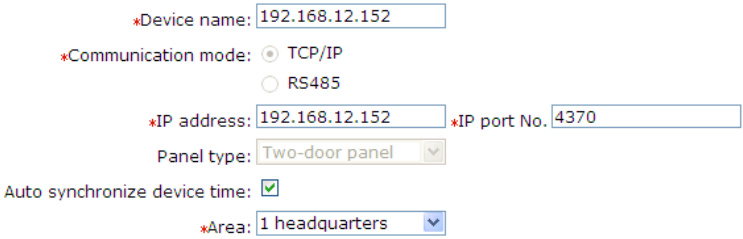
Synchronize all data: Synchronize all personnel in the same area with the device into the device. Select device, click [Synchronize all data] and click [OK] to complete synchronization.

Delete: Select device, click [Delete], and click [OK].

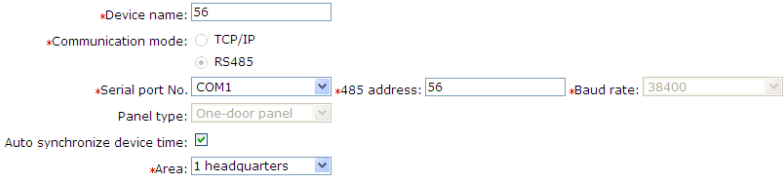
Edit: Click device name, or click [Edit] under “Related operation” behind the device

to pop up the edit interface.

If the communication mode is TCP/IP:



If the communication mode is RS485:

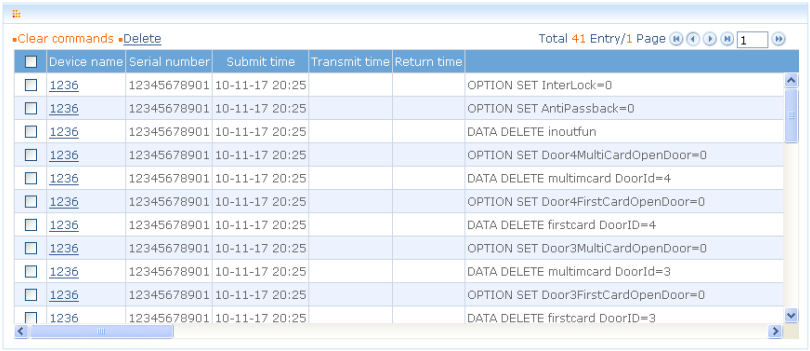


For the meanings and setting of the above parameters, see 4.2.1 Add access control panel. Communication method, IP address, IP port number, 485 address, baud rate, access control panel type and area are not editable. Device name can not be identical with the name of another device. Since device type cannot be modified, if the type is wrong, the user need manually delete the device and add it again.

5.3 Device Communication Management

1. Commands sent by server

Shows the list of commands sent to the device by the current system. If the return value is ≥0, execution is successful. If it is a negative, the execution failed.

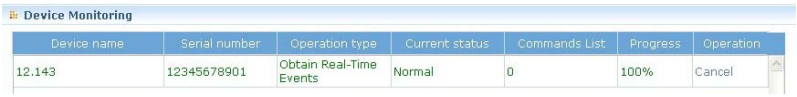

Clear commands Delete
Total 41 Entry/1 Page 1
Device name Serial number Submit time Transmit time Return time
1236 12345678901 10-11-17 20:25 OPTION SET InterLock=0
1236 12345678901 10-11-17 20:25 OPTION SET AntiPassback=0
1236 12345678901 10-11-17 20:25 DATA DELETE inoutfun
1236 12345678901 10-11-17 20:25 OPTION SET Door4MultiCardOpenDoor=0
1236 12345678901 10-11-17 20:25 DATA DELETE multimcard DoorId=4
1236 12345678901 10-11-17 20:25 OPTION SET Door4FirstCardOpenDoor=0
1236 12345678901 10-11-17 20:25 DATA DELETE firstcard DoorID=4
1236 12345678901 10-11-17 20:25 OPTION SET Door3MultiCardOpenDoor=0
1236 12345678901 10-11-17 20:25 DATA DELETE multimcard DoorId=3
1236 12345678901 10-11-17 20:25 OPTION SET Door3FirstCardOpenDoor=0
1236 12345678901 10-11-17 20:25 DATA DELETE firstcard DoorID=3

Clear command list: Click it to pop up the Confirm interface. Click [OK] to clear all items in the list of commands sent by the server;

Delete: Tick the check box before the command to be deleted, and click [Delete]. Confirm to delete the command.

2. Device monitoring

By default it monitors all devices with the current user's level, and lists the operation information of the devices: device name, serial number, operation type, current status, commands to be executed, and progress, etc.


Device Monitoring
Device name Serial number Operation type Current status Commands List Progress Operation
12.143 12345678901 Obtain Real-Time Events Normal 0 100% Cancel

6. Security System Management

1. Work principle of the access control system:

ZKAccess4.0 Security System is a WEB-based management system, realizing normal access control functions, management of networked access control panel via computer, and unified personnel access management.

The access control system can set the opening levels of registered users, namely, allowing some personnel to open some doors by verification during a time period.

It facilitates the management and support of multiple databases, including MySQL, SQL Server, and Oracle. Designed based on multi-business convergence, it supports service extension, such as attendance, patrol, and visitor management, etc., and supports multiple languages.

2. Access control system parameters:

- 256 time zones;
- 256 access levels;
- Three holiday types and totally 96 holidays;
- Anti-passback function;
- Interlock function;
- Linkage function;
- First-Card Normal Open function;
- Multi-Card Opening function;
- Remote door opening and closing;
- Real-time monitoring via Web browser;

3. Operation functions of access control system:

Click to enter the [Access Control System], and the main interface is [Real-time monitoring].

Access control system management primarily includes access control time zones, access control holiday, door settings, access levels, personnel access levels, real-time monitoring, and reports, etc.

6.1 Access control time zones

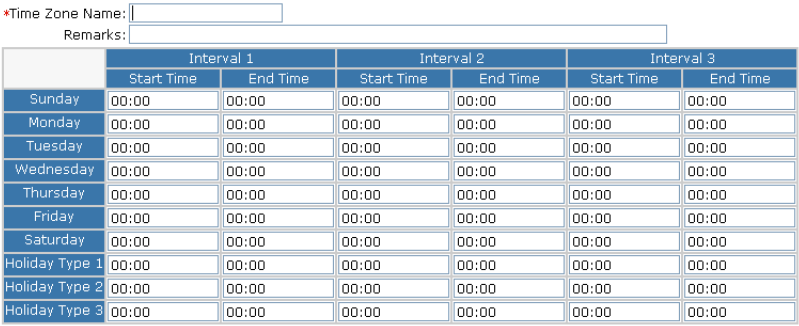
Access control time zone can be used for door timing. The reader can be made usable during valid time periods of certain doors and unusable during other time periods. Time zone can also be used to set Normal Open time periods of doors, or set access control levels so that specified users can only access specified doors during specified time periods (including access levels and First-Card Normal Open settings).

The system controls access according to access control time zones. The system can define up to 255 time zones. For each time zone, you can define, in a week, up to three intervals for each day and three holiday types. Each interval is the valid interval in 24 hours of each day. The format of each interval for a time zone: HH: MM-HH: MM, which is accurate to minutes in the 24-hour system.

Initially, the system, by default, has access control time zone named [Accessible 24 hours]. This time period can be modified but can not be deleted. The user can add access control time zones, which can be modified.

1. Add access control time zone:

(1) Click [Access Control System] - [Time zones] - [Add] to access the time zone setting interface;


*Time Zone Name:
Remarks:

	Interval 1		Interval 2		Interval 3	
	Start Time	End Time	Start Time	End Time	Start Time	End Time
Sunday	00:00	00:00	00:00	00:00	00:00	00:00
Monday	00:00	00:00	00:00	00:00	00:00	00:00
Tuesday	00:00	00:00	00:00	00:00	00:00	00:00
Wednesday	00:00	00:00	00:00	00:00	00:00	00:00
Thursday	00:00	00:00	00:00	00:00	00:00	00:00
Friday	00:00	00:00	00:00	00:00	00:00	00:00
Saturday	00:00	00:00	00:00	00:00	00:00	00:00
Holiday Type 1	00:00	00:00	00:00	00:00	00:00	00:00
Holiday Type 2	00:00	00:00	00:00	00:00	00:00	00:00
Holiday Type 3	00:00	00:00	00:00	00:00	00:00	00:00

The parameters are as follows:

Time zone name: Any character, up to a combination of 30 characters;

Remarks: Detailed description of the current time zone, including the explanation of the current time zone and primary applications, facilitating the user or other users with same level to view time zone information, which is up to 70 characters;

Interval and start/ end time: One access control time zone includes 3 intervals for

each day in a week, and three intervals for each of the three access control holidays. Set the start and end time of each interval;

Setting: If the interval is Normal Open: Just enter 00:00-23:59 as the first interval, and 00:00-00:00 as the second and third intervals. If the interval is Normal Close: All are 00:00-00:00. If only using one interval, the user just need to fill out the first interval (such as: Normal Open), and the second and third intervals will use the default value of 00:00-00:00. Similarly, when the user only uses the first two intervals, the third interval will use the default value of 00:00-00:00. When using two or three intervals, the user needs to ensure two or three intervals have no time intersection, and the time shall not span days. Otherwise, the system will prompt error.

Holiday Type: There are three holiday types in the time zone, they are unrelated to which day in week it is. If certain date is set to certain holiday type, the three intervals of the holiday type will be used for access. The holiday type in a time zone is optional. However, if the user does not fill out, the system will give the default value.

For example, refer to the figure above, set the access control interval of holiday type 1 as 8-20, the access control time period of holiday type 2 as Normal Open, and the access control time zone of holiday type 3 as Normal Close.

(2) After time zone setting, click [OK] to save, and the time zone will appear in the list.

2. Maintenance of access control time zone:

Edit: In the time zone list, click [Edit] button under “Related operation” to access time zone modification interface, and modify time zone setting. After modification, click [OK], and the modified time zone will be saved and shown in the time zone list.

Delete: In the time zone list, click [Delete] button under ”Related operation”. Click [OK] to delete the time zone, or click [Cancel] to cancel the operation. The time zone in use can not be deleted.

Tick the check boxes before one or more time zones in the time zone list. Click the [Delete] button over the list, and click [OK] to delete the selected time zones, or click [Cancel] to cancel the operation.

6.2 Access control holidays

The access control time of a holiday may differ from that of a weekday. For easy operation, the system provides holiday settings to set access control time for holidays.

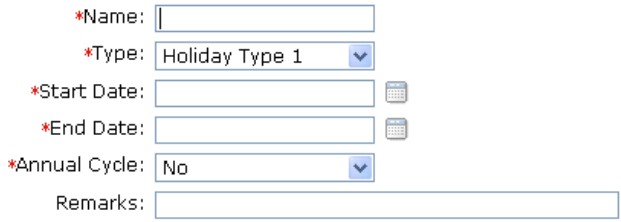
Access control holiday management includes add, modify and Delete access control holiday.

1. Add access control holiday:

Three holiday types are supported, each including up to 32 holidays. To conduct special access level configuration on special dates, the user can select special holidays for setting.

The operation steps are as follows

(1) Click [Access Control System] - [Holidays] - [Add] to access add access control holiday edit interface:



The fields are as follows:

Holiday Name: Any character, up to a combination of 30 characters;

Holiday Type: Holiday type 1/2/3, namely, a holiday record currently added is belong to these three holiday types, and each holiday type includes up to 32 holidays;

Start/ End Date: Must meet the date format as “2010-1-1”. The start date can not be later than the end date. Otherwise, the system will prompt error. the year of the start date can not be earlier than the current year, and the holiday can not span years;

Annual Cycle: Yes or No. The default is “No”. Annual cycle means that a holiday does not require modification in different years. For example, the Near Year’s Day is on January 1 each year, and can be set as “Yes”. For another example, the Mother's Day is on the second Sunday of each May, so its date is not fixed, and should be set as “No”;

For example, the date of the holiday “Near Year’s Day” is set as January 1, 2010, and the holiday type is 1, then on January 1, access time control will not follow the time of “Friday” in week, but the access control time of holiday type 1, such as the access time control between 8-20 in 7.1 Access control time zones.

(2) After editing, click [OK] button to save, and it will appear in the holiday list.

2. Modification of access control holiday:

To modify the original access control holiday, click [Edit] behind the access control holiday to access edit interface. After modification, click [OK] to save and quit.

3. Deletion of access control holiday:

In the access control holiday list, click [Delete] button under "Related operation". Click [OK] to delete the holiday, or click [Cancel] to cancel the operation. An access control holiday in use can not be deleted.

Tick the check boxes before one or more holidays in the holiday list. Click the [Delete] button over the list, and click [OK] to delete the selected holiday, or click [Cancel] to cancel the operation.

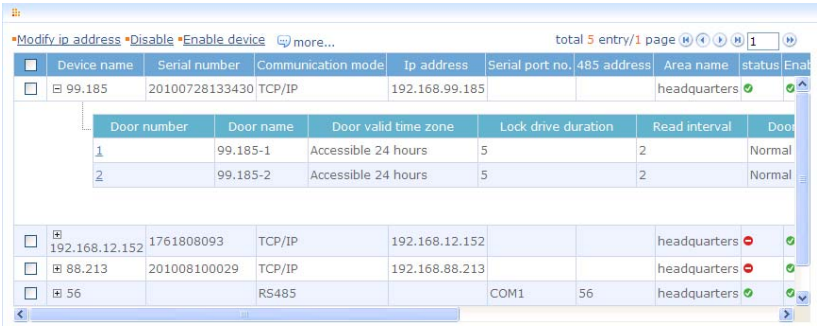
6.3 Door settings

Currently the system supports the connection and control of up to 50 access control panels.

The access control system is primarily for the management of personnel forbidden and admission. For security, a company will set personnel admission time zones, forbidden time zones and combinations of time zones. For door opening verification, First-Card Normal Open, Multi-Card Opening, anti-passback, linkage, and interlock can be set to enhance security. This system can provide real-time monitoring of doors and output of exception, access control events and access level reports.

6.3.1 Door management

Click [Access Control System] - [Door configuration], and by default it will access [Door management] interface, showing the list of all control panels. When unfolded, it can show all doors under the control of the control panel. Upon first entry into the access interface or successful query, if currently the system has access control panels or the query result is not null, by default it will unfold the doors of the first access control panel. Click corresponding button for relevant parameter setting.



Door management operations include: control panel management and door management.

1. Access Control panel operation

For communication between the system and the device, data uploading, configuration downloading, device and system parameters shall be set. The user can see access control panels within his levels in the current system, and can edit the devices here. If the user needs to add or delete devices, operate in device management.

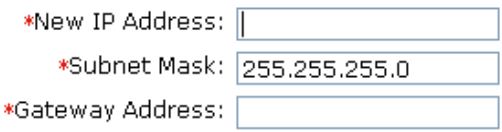
Control panel management includes: Modify IP address, disable, enable, modify communication password, synchronize time, upload event record, and upgrade firmware.

(1) Device profile:

Select device, click [Edit] under "Related operation". For Related details, see 5.2.3 Device maintenance.

(2) Modify IP address:

Select device, and click [Modify IP address] to show the modification interface. Enter new IP address, gateway, and subnet mask. Click [OK] to save settings and quit. This function is same as [Modify IP address function] in 5.2.2 Access control device. The difference is when searching control panels, the devices have not been added into the system, while the current [Modify device IP address] is regarding added devices.



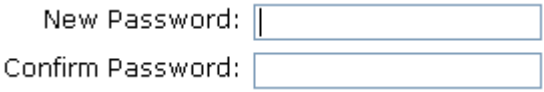
(3) Disable/Enable :

Select device, click [Disable/ Enable] to stop/ start using the device. When the device's communication with the system is interrupted or the device fails, the device may automatically appear in disabled status. At this time, after adjusting Internet or device, click [Enable device] to reconnect the device and restore device communication.

Note: If the current device is in enabled status and the connection is not successful, and the user conducts enable operation, the system will immediately reconnect the device.

(4) Modify communication password:

Enter the same new password for twice, and click [OK] to modify the communication password.



(5) Synchronize time:

Synchronize device time with current server time.

(6)Get event record:

Get real-time event records in the device into the system.

When the network status is normal and the communication status between the system and the device is normal, the system will acquire event records in the device in real-time and save them into system database. However, when the network is interrupted or communication is interrupted for some reasons, and the event records in the device have not been uploaded into the system in real-time, this operation can be used to manually acquire event records in the device. In addition, the system, by default, will automatically acquire event records in the device at 00:00 each day.

(7) Upgrade firmware

To upgrade firmware in the device, tick the device for which you want to upgrade firmware, click [Upgrade firmware], enter edit interface, click [Browse] to select the firmware upgrade file (named emfw.cfg) provided by us, and click [OK] to start upgrading.

Note: The user shall not upgrade firmware without authorization. Contact the distributor before upgrading firmware, or upgrade it when instructed by the

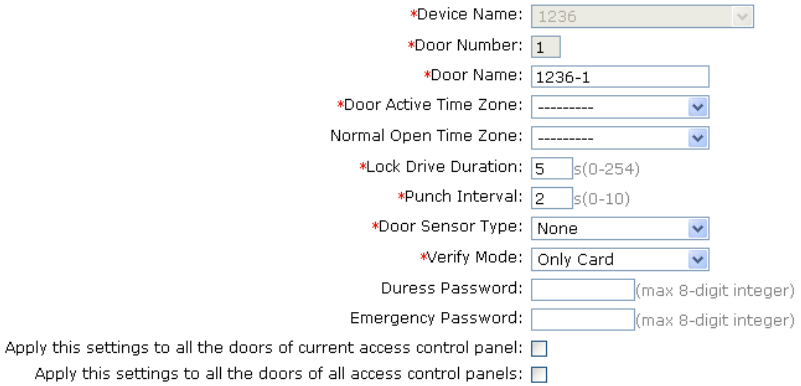
distributor. Unauthorized upgrading may bring problems that affect your normal use.

2. Door management:

The device list will show all access control devices. Click the "+" button before the device name to show the door list under a device. When adding device, it will automatically add doors (corresponding device name and door numbers can not be edited) according to the number of doors. Before using the device (including doors), the user must edit door information one by one (or apply current settings to other doors). After editing, they will be sent to the device, which can be used after successful setting.

(1) Door parameter modification:

Select the door to be modified, and click [Edit] under "Related operation" to show the Edit interface;


*Device Name: 1236
*Door Number: 1
*Door Name: 1236-1
*Door Active Time Zone: ---------
Normal Open Time Zone: ---------
*Lock Drive Duration: 5 s(0-254)
*Punch Interval: 2 s(0-10)
*Door Sensor Type: None
*Verify Mode: Only Card
Duress Password: (max 8-digit integer)
Emergency Password: (max 8-digit integer)
Apply this settings to all the doors of current access control panel:
Apply this settings to all the doors of all access control panels:

The fields are as follows:

Device Name: It is not editable (need to be edited in 5.2.1 Add access control panel);

Door Number: The system automatically name the numbers of doors according to how many doors of the device (for example, the four doors of a four-door control panel are numbered 1, 2, 3 and 4). The number will be consistent with the door number on the device.

Note: Although by default the number following the underline in the door name is consistent with the door number, but 1/2/3/4 in anti-passback and interlock refers to door serial number rather than the number following the door name, and

they have no necessary relation, and the system allows the user to modify the door name, so they can not be confused;

Door Name: The default door name is "device name_door number". The field allows the user to modify as required. Up to 30 characters can be entered;

Door Active Time Zone, **Normal Open Time Zone**: By default either is null. Initialized and added access control time zones will be shown for the user to select. Upon door editing, door valid time zone is need to input. Only after setting door valid time zone, the door can be opened and closely normally. We recommend to set door normal open time period within the door valid time zone, only in this situation, the door normal open time zone is valid;

Note: Consecutive punching of a card having access level of the door for 5 times can release the normal open status within one day (including First-Card Normal Open), and close the door immediately.

Lock Drive Duration: Used to control the delay for unlocking after card punching. The unit is second, and the default is 5 seconds. The user can enter a number between 0-254;

Punch Interval: The unit is second (range: 0-10 seconds), and the default is 2 seconds;

Door Sensor Type: NO (door sensor not detected), Normal Open, Normal Close. The default is NO. When editing doors, the user can select the door sensor type to be Normal Open or Normal Close. If Normal Open or Normal Close is selected, it is required to select **door status delay** and whether **close and reverse-lock** is required. By default, once door sensor type is set as Normal Open or Normal Close, the default door status delay will be 15s, and by default it will enable close and reverse-lock.

Door Status Delay: The duration for delayed detection of door sensor after the door is opened. Detection is performed only after the door is opened and the delay duration expired. When the door is not in the "Normally Open" period, and the door is opened, the device will start timing. It will trigger alarm when the delay duration expired, and stop alarm when you close the door. The default door status delay will be 15s. The **door status delay** should be longer than **lock drive duration**.

Close and Reverse-lock: Set locking or not after door closing. Tick it for lock after door closing.

Verify Mode: Supports Only Card and Card Plus Password verify modes. The default is Only Card. When Card Plus Password mode is selected, make sure the door uses a reader with keyboard;

Duress Password, **Emergency Password**: Upon duress, use duress password (used with legally card) to open the door. When opening the door with duress password, it will alarm. Upon emergency, the user can use emergency password (named super password) to open the door. Emergency password allows normal door opening. Emergency password is effective in any time zone and any type of verify mode, usually used for the administrator.

Duress Password Opening (used with legally card): When Only Card verify mode is used, you need press [ESC] first, and then press the setting password plus [OK] button, finally swipe your card, the door open and trigger the alarm. When Card Plus Password verify mode is used, please swipe your card first, then press the password number plus [OK] button (same to normal door open in card plus password verify mode), the door open and trigger the alarm.

Emergency Password Opening: The password must be a number not exceeding 8 digits (integer). The door can be opened just by entering the password. Please press [ESC] every time before entering password, and then press OK to execute.

When using duress password or emergency password, the interval for entering each number shall not exceed 10 seconds, and these two number should not be the same.

Apply this settings to all the doors of current access control panel: Click to apply to all doors of the current access control panel;

Apply this settings to all the doors of all access control panels: Click to apply to all doors of all access control panels within the current user's level;

After parameter editing, click [OK] to save and quit.

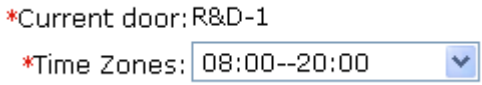
6.3.2 First-Card Normal Open

First-Card Normal Open: During a specified interval, after the first card punching by a person having First-Card Normal Open level, the door will be Normal Open, and will automatically restore closing after the valid interval expired.

The user can set First-Card Normal Open for a specific door. The settings include door, door opening time zone and personnel with First-Card Normal Open level. A door can have First-Card Normal Open settings for multiple time zones. The interface of each door will show the number of existing First-Card Normal Open settings. For First-Card Normal Open setting, when adding or editing each record, it is not required to modify the "current door", but to select time zone. When record adding is successful, add personnel that can open the door for a First-Card Normal Open setting record. On the right of the interface, you can browse door opening personnel in a First-Card Normal Open setting and delete current personnel, so that some personnel will not have First-Card Normal Open level any more.

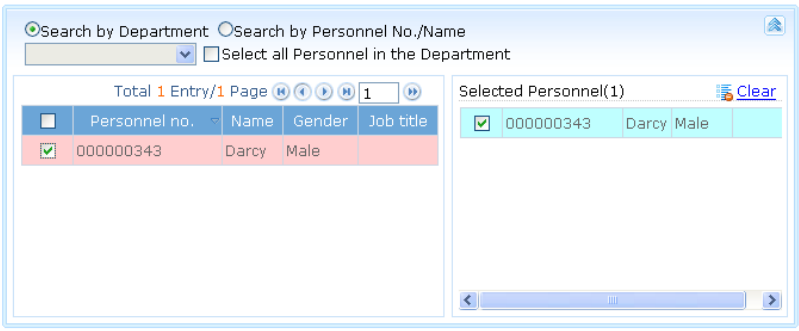
The operation steps are as follows:

1. Click [Settings] under “First-Card Normal Open” of a door to show First-Card Normal Open setting interface;

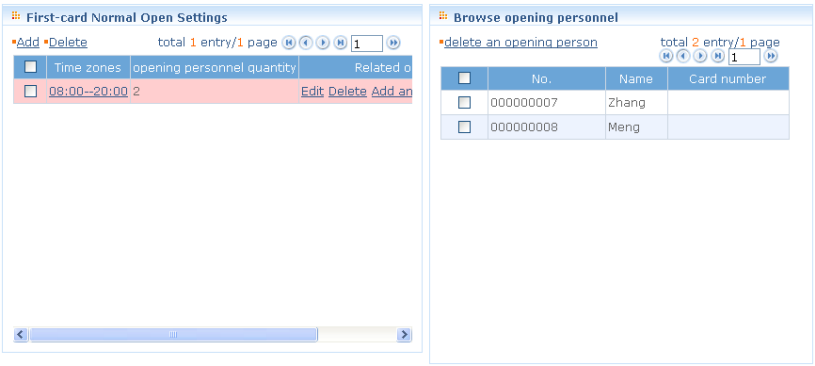


2. Click [Add], select the time zone of First-Card Normal Open, and click [OK] to save the settings;

3. Click [Add personnel] under “Related operation” to set personnel having First-Card Normal Open level.



Click [OK] to save and quit editing, the following interface appears.



Note: For a door currently in Normal Open time period, consecutive punching of a card having access level for the door for 5 times(the card punching interval should within 5 second.) can release the current Normal Open status and close the door.The sixth card punching will be a normal card punching. This function only effective at the door valid time zone. Normal Open intervals set for other doors within the day and First-Card Normal Open settings will not take effect anymore.

6.3.3 Multi-Card Opening

1. Multi-Card Opening Personnel Groups:

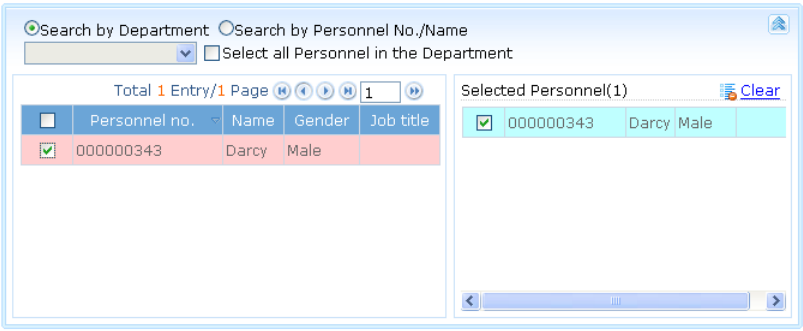
It is a personnel grouping. The group will be used for the setting of Multi-Card Opening.

(1) Click [Access Control System] - [Door Configuration] - [Multi-Card Opening Personnel Groups] - [Add] to show the following edit interface:

Group name: Any character, up to a combination of 30 characters, which can not be identical with an existing group name;

After editing, click [OK], return and the added Multi-Card Opening Personnel Groups will appear in the list;

(2) Select a group, and click [Add personnel] to add personnel to the group:



(3) After selecting and adding personnel, click [OK] to save and return.

Note: One person can only belong to one group, and can not be grouped repeatedly.

2. Multi-Card Opening:

Set levels for personnel in [Multi-Card Opening Personnel Groups].

This function needs to be enabled in some special access occasions, where the door will open only after consecutive card punching by several people. Before verifying, any card punching out of this combination (even the card belong to other combination) will interrupt the procedure, and you need to wait 10 seconds to restart verifying. It will not open upon card punching by one of the combination.

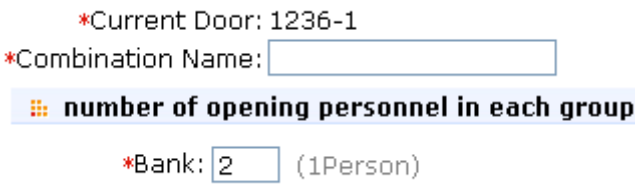
If currently [Multi-Card Opening Personnel Groups] is not configured, the system will prompt, and the user can only add combination name. The system permits the user to add a name-only combination, and to edit Multi-Card Opening combination when [Multi-Card Opening Personnel Groups] is added.

Multi-Card Opening combination is a combination of the personnel in one or more Multi-Card Opening Personnel Groups. When setting the number of people in each group, you can configure one group (such as combined door opening by two people in one group) or multiple groups (such as combined door opening by four people, including 2 people in group 1 and 2 people in group 2), and at least one group shall be entered a number of door opening people not being 0, and meanwhile the total number of door opening people shall not be greater than 5. In addition, if the number of people entered by the user is greater than the number of people in the current group, the Multi-Card Opening function will be unable to be realized normally.

Multi-Card Opening settings:

(1) Click [Access Control System] - [Door configuration] - [Door management], click [Setting] under “Multi-Card Opening” of a door in the door list to show the Multi-Card Opening setting interface;

(2) Click [Add] to pop up Add Multi-Card Opening setting interface;



(3) For Multi-Card Opening, the number of people for combined door opening is up to 5. What in the brackets is the current actual number of people in the group. Set the

number of people for combined door opening in a group, and click [OK] to complete editing.

6.3.4 Interlock settings

Interlock can be set for any two or more lock belong to one access control panel, so that when one door is opened, the others will be closed. And you can open one door only when others are closed.

Add interlock settings:

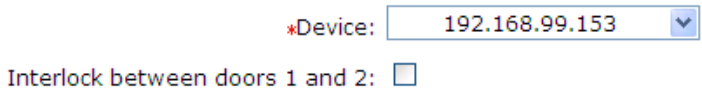
1. Click [Access Control System] - [Door configuration] - [Interlock settings] - [Add] to enter the interlock setting edit interface;

2. Select device to show interlock settings. Since one device can only correspond to one interlock setting record, when adding, interlocked devices can not be seen in the dropdown list of the device. When deleting established interlock information, the corresponding device will return to the dropdown list. The setting page will vary with the number of doors controlled by the selected device:

A one-door control panel has no interlock settings;

A two-door control panel: 1-2 two-door interlock settings;

A four-door control panel: 1-2 two-door interlock, 3-4 two-door interlock, 1-2-3 three-door interlock, 1-2-3-4 four-door interlock;



3. Select interlock settings, tick an item (multiple interlocks can be selected as long as doors are not repeated), click [OK] to complete setting, and then the added interlock settings will be shown in the list.

For example, select 1-2-3-4 four-door interlock, if you want open door 3, doors 1, 2 and 4 need to be closed.

Note: When editing, the device can not be modified, but the interlock setting can be modified. If interlock setting is not required for the device any more, the interlock setting record can be deleted. When deleting a device record, its interlock setting record, if exist, will be deleted.

6.3.5 Anti-passback settings

Currently anti-passback settings support in and out anti-passback. In some special occasions, it is required that the card holder who entered from a door by card punching must exit from the same door by card punching, with the entry and exit records strictly consistent. One who followed another to enter the door without card punching will be denied when trying to exit by card punching, and one who followed another to exit without card punching will be denied when trying to enter by card punching. And when one who entered by card punching gives the card to another to try entering, the other person will be denied. The user can use this function just by enable it in the settings. This function is normally used in prisons, the army, national defense, scientific research, bank vaults, etc.

Add anti-passback settings:

1. Click [Access Control System] - [Door configurations] - [Anti-passback settings] - [Add] to show anti-passback setting edit interface;

2. Select device (N-door control panel), because one device can only correspond to one anti-passback setting record, so when adding, devices with anti-passback settings cannot be seen in the dropdown list. When deleting established anti-passback information, the corresponding device will appear in the dropdown list. The settings vary with the number of doors controlled by the device:

For one-door two-way and two-door two-way control panels, anti-passback between readers and between doors can be set. For two-door one-way and four-door one-way control panels, only anti-passback between doors can be set. The card holder enter from door A, he must exit from door B, this function is used for channel or ticket management.

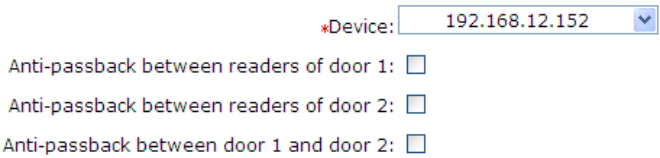
Anti-passback settings (two-way) of one-door control panel: anti-passback between readers;

Anti-passback settings (two-way) of a two-door control panel:

Anti-passback between readers of door 1, anti-passback between readers of door 2, anti-passback between respective readers of doors 1/2, anti-passback between doors 1/2;

Anti-passback settings of a four-door control panel:

Anti-passback of doors 1-2, anti-passback of doors 3-4, anti-passback of doors 1/2-3/4, anti-passback of doors 1-2/3, anti-passback of doors 1-2/3/4;


*Device:
192.168.12.152
Anti-passback between readers of door 1:
Anti-passback between readers of door 2:
Anti-passback between door 1 and door 2:

3. Select anti-passback settings, and tick one item (anti-passback without repetition of doors or readers can be subject to multi-choice), click [OK] to complete setting, and the added anti-passback settings can be shown in the list.

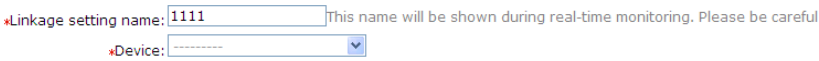
Note: When editing, you can not modify the device, but can modify anti-passback settings. If anti-passback setting is not required for the device any more, the anti-passback setting record can be deleted. When deleting a device record, its anti-passback setting record, if exist, will be deleted.

6.3.6 Linkage setting

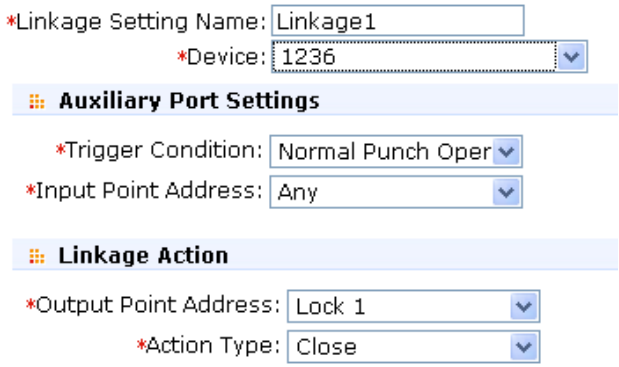
Linkage setting means when an event is triggered at an input point of the access control system, a linkage action will occur at the specified output point to control such events as verification, opening, alarm and exception of the system and list them in the corresponding monitored report for view by the user.

Add linkage setting:

1. Click [Access Control System] - [Door configurations] - [Linkage setting] - [Add] to show the linkage setting interface;



2. Input linkage setting name (input linkage setting name before selecting device). After selecting device, corresponding linkage setting will appear (The system will first determine whether or not the device is successfully connected and has read extended device parameters such as auxiliary input quantity, auxiliary output quantity, door quantity and reader quantity. If the system has no available extended device parameters, it will remind the user of failing to set anti-passback. Otherwise, it will, shows linkage setting options according to the currently selected device, such as the door quantity, auxiliary input and output quantity):



The fields are as follows:

Trigger Condition: Normal Punch Open, Punch during Normal Open Time Zone, First Card Normal Open Punch, Multi-Card Open, Emergency Password Open, Open during Normal Open Time Zone, Linkage Event Triggered, Cancel Alarm, Remote Opening, Remote Closing, Cancel Normal Open, Too Short Punch Interval, Punch during Invalid Time Zone, Illegal Time Zone, Illegal Access, Anti-Passback, Interlock, Multi-Card Authentication, Unregistered Card, Opening Timeout, Card Expired, Duress Password Open, Opened Accidentally, Opened, Closed, Exit Button Open, Auxiliary Input Point Disconnected, Auxiliary Input Point Shorted.

Input Point Address: Any, Door 1, Door 2, Door 3, Door 4, Auxiliary Input 1, Auxiliary Input 2, Auxiliary Input 3, Auxiliary Input 4, Auxiliary Input 9, Auxiliary Input 10, Auxiliary Input 11, Auxiliary Input 12 (the specific input point please refer to specific device parameters);

Output point address: Lock 1, Lock 2, Lock 3, Lock 4, Auxiliary Output 1, Auxiliary Output 2, Auxiliary Output 3, Auxiliary Output 4, Auxiliary Output 6, Auxiliary Output 8, Auxiliary Output 9, Auxiliary Output 10 (the specific output point please refer to specific device parameters);

Action Type: Close, Open, Normal Open. By default it is closed. To open, delay time shall be set, or Normal Close can be selected;

Delay: Ranges from 1-254s (This item is valid when the action type is Open)

3. After editing, click [OK] to save and quit, and the added linkage setting will be shown in the linkage setting list.

For example: If select “Normal Punching Card Open” as the trigger condition, and the input point is Door 1, the output point is Lock 1, the action type is Open, the

delay is 60s, then when “Normal Punching Card Open” occurs at Door 1, the linkage action of “Open” will occur at Lock 1, and door will be open for 60s.

Note: When editing, you can not modify the device, but can modify linkage setting name and configuration. When deleting a device, its linkage setting record, if exist, will be deleted.

If system has set that the input point is a specific door or auxiliary input point under a trigger condition of a device, it will not allow the user to add (or edit) a linkage setting record where the device and trigger condition are the same but the input point is ‘Any’.

On the contrary, if the device and trigger condition are the same, and the system has linkage setting record where the trigger point is ‘Any’, the system will not permit the user to add (or edit) a linkage setting record where the input point is a specific door or auxiliary input.

In addition, the system does not allow the same linkage setting at input point and output point in specific trigger condition.

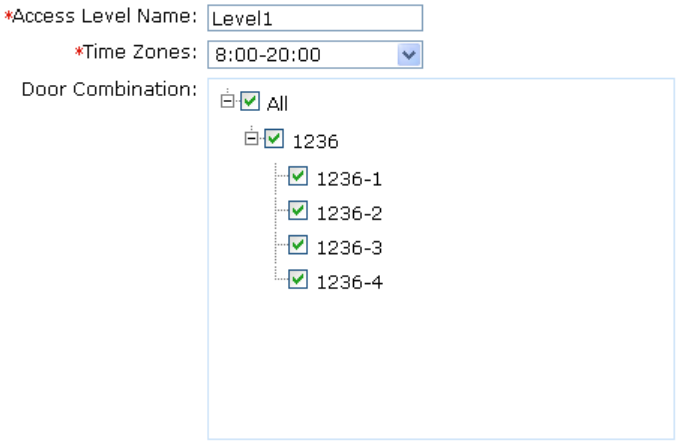
The same device permits consecutive logical (as mentioned above) linkage settings.

6.4 Access levels

Access levels means in a specific time period, which door or door combination can be opened through verification. However, the personnel combination that can open these doors via verification shall be set in personnel access levels settings. Please refer to 6.5 Personnel access levels settings.

Add access levels:

1. Click [Access Control System] - [Access levels] - [Add] to enter Add access levels edit interface;



2. Set parameters: access level name (no repetition), access control time zones, door combination;

3. Click [OK] to complete setting and quit, and added access levels will appear in the list.

Note:

(1) Select the doors in the access levels as multi-choice, so you can select different doors in different control panels;

(2) Two levels with the same time zone and door combination are not allowed in the system.

6.5 Personnel access levels

To assign access levels for the personnel to verify and get through, personnel access levels have two display modes:

Display as levels: Add/delete personnel for specific access levels.

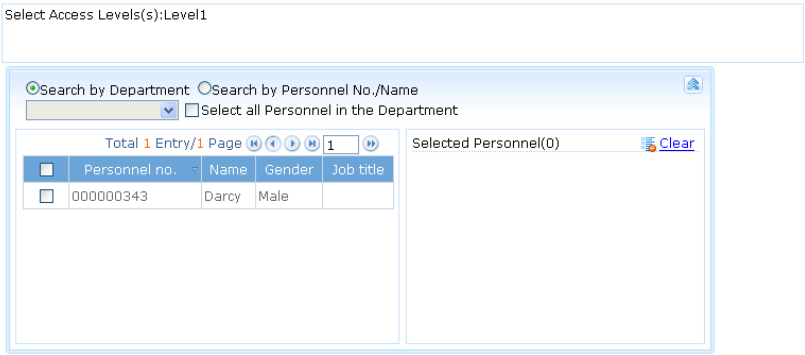
Display as personnel: Add specified personnel into specified access levels, or delete specified personnel from specified access levels;

1. Add/delete personnel to levels:

(1) Click [Access Control System] - [Personnel access levels] - [Shown by Access levels], and click a level, then personnel having opening levels in the access level

will be shown in the list on the right;

(2) Click [Add personnel] to pop up the Add personnel interface,



Select personnel to create the list on the right, and click [OK] to complete adding, and added personnel will appear in the list on the right;

(3) Select personnel, click [Delete from access level] to delete the personnel from the access level.

Note: When adding personnel, if selected personnel exist in the current access level, the system can not add again.

2. Edit access level for personnel:

(1) Click [Access Control System] - [Personnel access level settings] - [Shown by personnel] interface, click a person, and the list on the right will show the access level of the person;

(2) Click [Add access level] to pop up edit interface, select access level, click [OK] to complete editing, and the list on the right will show the access level;

(3) Select access level, and click [Delete access level] to the person from the access level.

6.6 Real-time monitoring

Monitor the statuses and real-time events of doors under the access control panels in the system in real-time, including normal events and exceptional events (including alarm events).

1. Monitoring all :

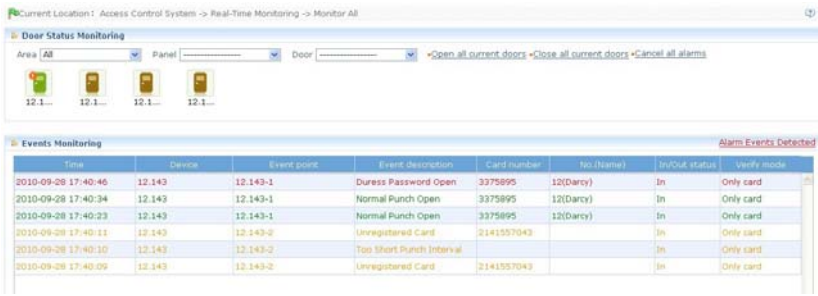
The system will, by default, show the monitoring of all doors under the control panels within the current user's access level. The user can monitor one (or more) door(s) by [Area], [Control panel] or [Door].

Open all current doors: Open all doors currently shown;

Close all current doors: Close all doors currently shown.

Cancel all alarms: Once alarming doors appear on the interface, the system will alarm. Click to cancel the alarms of the control panels for alarming doors. If Cancel Alarms is successful, the system will automatically stop alarming.

Note: If a control panel have multiple door alarms at the same time, you need only execute one cancel operation at one of these door to cancel all the alarm in this control panel.


Current Location: Access Control System -> Real-Time Monitoring -> Monitor All
Door Status Monitoring
Area All
Panel
Door
Open all current doors
Close all current doors
Cancel all alarms
Events Monitoring
Alarm Events Detected
Time
Device
Event point
Event description
Card number
No.(Name)
In/Out status
Verify mode
2010-09-28 17:40:46 12.143 12.143-1 Duress Password Open 3375895 12(Darcy) In Only card
2010-09-28 17:40:34 12.143 12.143-1 Normal Punch Open 3375895 12(Darcy) In Only card
2010-09-28 17:40:23 12.143 12.143-1 Normal Punch Open 3375895 12(Darcy) In Only card
2010-09-28 17:40:11 12.143 12.143-2 Unregistered Card 2141557043 In Only card
2010-09-28 17:40:10 12.143 12.143-2 Too Short Punch Interval In Only card
2010-09-28 17:40:09 12.143 12.143-2 Unregistered Card 2141557043 In Only card

Upon Door Status Monitoring, if the number of doors on the current interface <=64, the system will, by default, show the doors in pictures to monitor door statuses. Once the number exceeds 64, the system will automatically list the doors.

When putting the cursor on a door, it will show relevant parameters and operations: device, door number, door name, remote opening, and remote closing. Icons in different colors represent statuses as follows:

Icon						
Status	Door alarming	Door closed when online	Door opened when online	Door sensor unset	Door offline	Door opening timeout

Event monitoring:

The system automatically acquires monitored device event records, including normal access control events and exceptional access control events (including alarm events). Alarm events appear in red. Exceptional events excluding alarm events appear in orange. Normal events appear in green.

Meanwhile, when an alarm event record appears on the event monitoring interface, the “Find alarm event” prompt will appear on the upper right corner. After the user clicks the link, the system will redirect to the alarm event monitoring interface by opening a new window (or tab page).

On the current event monitoring interface, the recent records are on the top, enabling the user to see without dragging the scrollbar. Meanwhile, the interface will show up to some 100 records.

The list is shown below.

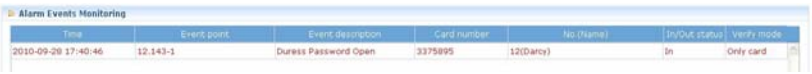
Click [Find alarm event] on the upper right corner to access [Alarm event] interface, and the user will see alarm events monitored in [Event monitoring] before page turn and alarm events after the current time point.

2. Alarm event:

Alarm event records are actually part of exception records, namely, alarm event records in exception records.

Alarm event monitoring only monitors alarm events acquired in system, and only monitors alarm events after the time of accessing the interface.

The alarm event monitoring list is shown below:



Appendix: Real-Time Event Description:

Normal Punch Open: Means the person has open door permission punch the card and trigger this normal event of open the door .

Punch during Normal Open Time Zone: At the normally open period (set to normally open period of a single door or the door open period after the first card normally open), the person has open door permission punch the effective card at the

opened door to trigger this normal events.

First Card Normal Open Punch: The person has first card normally open permission, punch card at the setting first card normally open period but the door is not opened, and trigger the normal event.

Multi-Card Open: Multi-card combination can be used to open the door. After the last piece of card verified, the system trigger this normal event.

Emergency Password Open: The password (also known as the super password) set for the current door can be used for door open. It will trigger this normal event after the emergency password verified.

Open during Normal Open Time Zone: If the current door is set a normally open period, the door will open automatically after the setting start time, and trigger this normal event.

Linkage Event Triggered: After the system linkage configuration take effect, trigger this normal event.

Cancel Alarm: When the user cancel the alarm of the corresponding door, and the operation is success, trigger this normal event.

Remote Opening: When the user open a door from remote and the operation is successful, it will trigger this normal event.

Remote Closing: When the user close a door from remote and the operation is successful, it will trigger this normal event.

Cancel Normal Open: Punch effective card 5 times or remote close the door to cancel the current state of the door normally open, trigger this normal event.

Too Short Punch Interval: when the interval between two card punching is less than the set time interval, trigger this abnormal event.

Punch during Invalid Time Zone: The user has the door open permission, punch card but not at the door effective period of time, and trigger this abnormal event.

Illegal Door Active Time Zone: The user has the door open permission, punch card but not at the access effective period of time, and trigger this abnormal event.

Access Denied: The registered card without the access permission of the current door, punch to open the door, trigger this abnormal event.

Anti-Passback: When the anti-pass back setting of the system take effect, trigger this abnormal event.

Interlock: When the interlocking rules of the system take effect, trigger this abnormal event.

Multi-Card Authentication: Use multi-card combination to open the door, the card verification before the last card (whether verified or not), trigger this normal event.

Unregistered Card: Refers to the current card is not registered in the system, trigger this abnormal event.

Opening Timeout: The door sensor detect that it is expired the delay time after opened, if not close the door, trigger this abnormal event.

Password Error: Use card plus password, duress password or emergency password to open the door, trigger this event if the password is wrong.

Card Expired: The person with the door access permission, punch card to open the door after the effective time of the access control, can not be verified and will trigger this abnormal event.

Duress Password Open: Use the duress password of current door verified and triggered alarm event.

Opened Accidentally: Except all the normal events (normal events such as user with door open permission to punch card and open the door, password open door, open the door at normally open period, remote door open, the linkage triggered door open), the door sensor detect the door is opened, that is the door is unexpectedly opened.

Door Opened Correctly: When the door sensor detect that the door has been properly opened, triggering this normal event.

Door Closed Correctly: When the door sensor detect that the door has been properly closed, triggering this normal event.

Exit Button Open: When using the door button to open the door, triggering this normal event.

Auxiliary Input Disconnected: When the auxiliary input point disconnected, trigger this normal event.

Auxiliary Input Shorted: When the auxiliary input point short circuit, trigger this normal event.

6.7 Access control reports

Includes [All access control events], [Access control exception events] and [Personnel access levels] reports. You can select Export all and Export after query.

The user can generate statistics of relevant device data from access control reports, including card verification information, door operation information, and normal card punching information, etc.

Normal event: Such as Normal Punch Open, Punch during Normal Open Time Zone, First Card Normal Open Punch, Multi-Card Open, Emergency Password Open, Open during Normal Open Time Zone, Linkage Event Triggered, Cancel Alarm, Remote Opening, Remote Closing, Cancel Normal Open, Opened, Closed, Exit Button Open, Auxiliary Input Point Disconnected, Auxiliary Input Point Shorted, etc.;

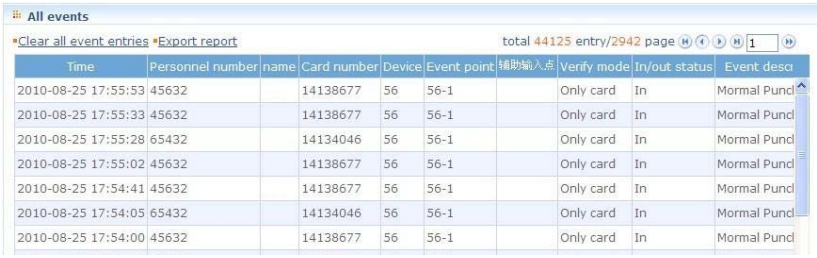
Exceptional Event: Such as Too Short Punch Interval, Punch during Invalid Time Zone, Illegal Time Zone, Illegal Access, Anti-Passback, Interlock, Multi-Card Authentication, Unregistered Card, Opening Timeout, Card Expired, , and Duress Password Open and Opened Accidentally are alarm events.

Verify mode: Only Card, Only Password, Card Plus Password and others.

Note: Only event records generated when the user uses emergency password to open doors will include [Only password] verification mode.

❁ All access control events

Because the data size of access control event records is large, you can view access control events as specified condition when querying. By default, the system shows the report of all access control events:


All events

Clear all event entries Export report

total 44125 entry/2942 page 1

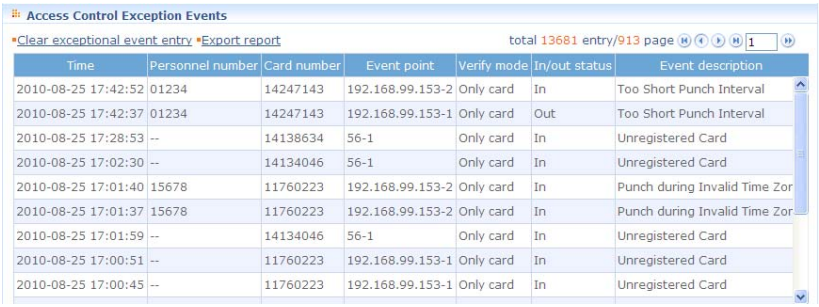
Time	Personnel number	name	Card number	Device	Event point	辅助输入点	Verify mode	In/out status	Event desc
2010-08-25 17:55:53	45632		14138677	56	56-1		Only card	In	Mormal Punch
2010-08-25 17:55:33	45632		14138677	56	56-1		Only card	In	Mormal Punch
2010-08-25 17:55:28	65432		14134046	56	56-1		Only card	In	Mormal Punch
2010-08-25 17:55:02	45632		14138677	56	56-1		Only card	In	Mormal Punch
2010-08-25 17:54:41	45632		14138677	56	56-1		Only card	In	Mormal Punch
2010-08-25 17:54:05	65432		14134046	56	56-1		Only card	In	Mormal Punch
2010-08-25 17:54:00	45632		14138677	56	56-1		Only card	In	Mormal Punch

Clear all event records:

Click [Clear all event records] to pop up a prompt. Click [OK] to clear records.

❁ Access control exception events

You can view access control exception events in specified condition. The options are same as those of [All access control events].



Time	Personnel number	Card number	Event point	Verify mode	In/out status	Event description
2010-08-25 17:42:52	01234	14247143	192.168.99.153-2	Only card	In	Too Short Punch Interval
2010-08-25 17:42:37	01234	14247143	192.168.99.153-1	Only card	Out	Too Short Punch Interval
2010-08-25 17:28:53	--	14138634	56-1	Only card	In	Unregistered Card
2010-08-25 17:02:30	--	14134046	56-1	Only card	In	Unregistered Card
2010-08-25 17:01:40	15678	11760223	192.168.99.153-2	Only card	In	Punch during Invalid Time Zor
2010-08-25 17:01:37	15678	11760223	192.168.99.153-2	Only card	In	Punch during Invalid Time Zor
2010-08-25 17:01:59	--	14134046	56-1	Only card	In	Unregistered Card
2010-08-25 17:00:51	--	11760223	192.168.99.153-1	Only card	In	Unregistered Card
2010-08-25 17:00:45	--	11760223	192.168.99.153-1	Only card	In	Unregistered Card

Clear access control exception event records: Clear the list of all access control exception events.

❁ Personnel access level

View all access levels and all personnel under each level. The list items include access level name, access control time period, and door combination:

Access level name	Time zones	Door combination	
TCP/IP	Accessible 24 hours	192.168.99.153-1,192.168.99.153-2,99.185-1,99.185-2	33333 ,44444 00231 55555 ,66666 ,4
485	Accessible 24 hours	56-1	4563265432,65432
IP	8	88.213-1	0012344444,0032144444,00231

7. System Settings

System settings primarily include assigning system users (such as company management personnel, registrar, access control administrator) and configuring the roles of corresponding modules, managing database, such as backup, initialization, and setting system parameters and operation logs, etc.

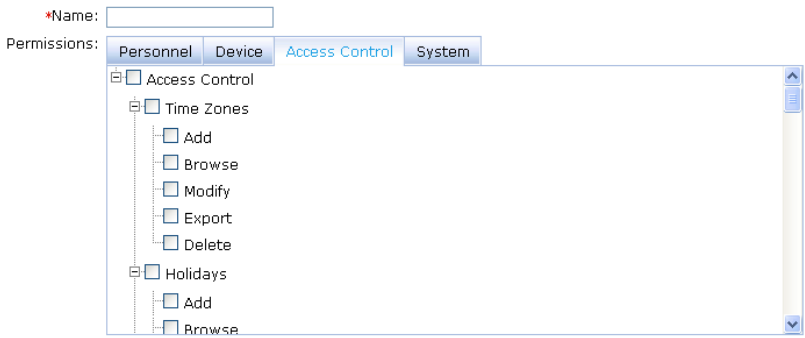
7.1 User management

1. Role management:

During daily use, the super user needs to assign new users having different levels. To avoid individual setting for each user, roles having certain levels can be set in role management, and then be assigned to specified users, including the levels set for five major functional modules of personnel, device, access control and system setting. The system's default super user has all levels, and can create new users and set corresponding levels as required.

Role setting steps:

(1) Click [Add] to enter role setting interface;



(2) Set name, select your desired role setting item, and tick levels to be configured for users of different levels;

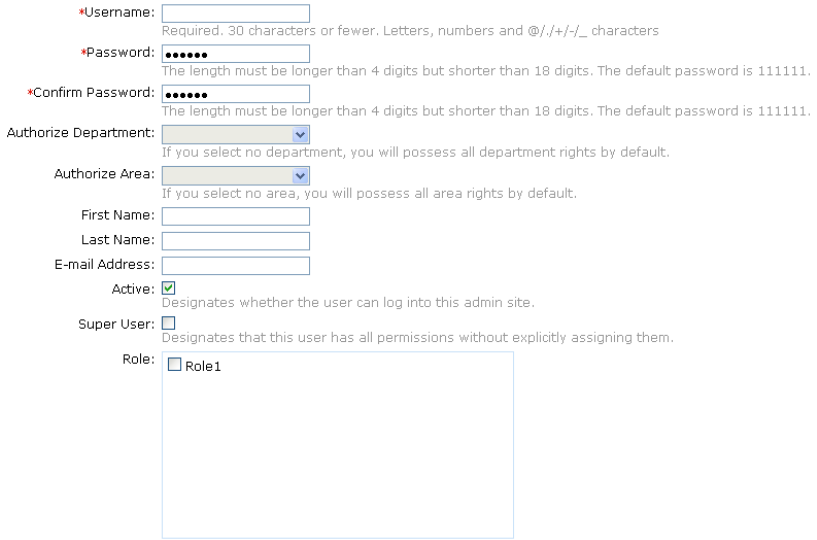
(3) After setting, click [OK] to save and return to the list, and added role settings will be shown in the list.

2. User management:

Add new users to the system, and assign user roles (levels).

Add user:

1. Click [Add], enter new user information, where items with [*] are mandatory. The parameters are as follows:


*Username:
Required. 30 characters or fewer. Letters, numbers and @/./+/-/_ characters
*Password:
The length must be longer than 4 digits but shorter than 18 digits. The default password is 111111.
*Confirm Password:
The length must be longer than 4 digits but shorter than 18 digits. The default password is 111111.
Authorize Department:
If you select no department, you will possess all department rights by default.
Authorize Area:
If you select no area, you will possess all area rights by default.
First Name:
Last Name:
E-mail Address:
Active:
Designates whether the user can log into this admin site.
Super User:
Designates that this user has all permissions without explicitly assigning them.
Role:
Role1

Username: Not more than 30 characters, only using letters, numbers or characters;

Password: The length must be more than 4 digits and less than 18 digits. The default password is 111111;

Authorize Department: If you select no department, you will possess all department rights by default;

Authorize Area: If you select no area, you will possess all area rights by default;

Enter **First Name**, **Last Name** and **E-mail Address**;

Active: Designates whether the user can log into the admin site. Tick to enable it;

Super User : Designates that this user has all permissions without explicitly assigning them. Tick it to be a super user without selecting a role;

Select Role: Non-super user needs to select a role. By selecting a preset role configuration, this user will have the levels configured for the role.

2. After editing, click [OK] to complete user adding, and the user will be shown in the list.

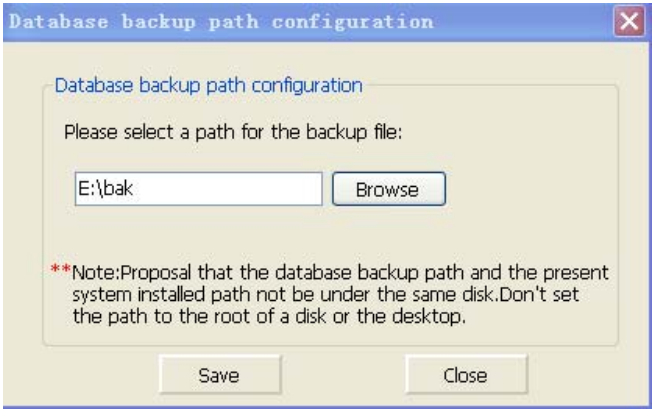
To modify existing user, click [Edit] behind the user name, and enter edit interface. After modification, click [OK] to save and return.

7.2 Database management

The homepage of the system shows database backup history. The system allows database backup, restoration and initialization.

1. Database backup path configuration:

Select [Database backup path configuration] in the [Server Controller] operation menu, the following interface appear.


Database backup path configuration
Database backup path configuration
Please select a path for the backup file:
E:\bak
Browse
**Note:Proposal that the database backup path and the present system installed path not be under the same disk.Don't set the path to the root of a disk or the desktop.
Save
Close

Click [Browse] to select the backup path, click [Save] to save the selection and quit.

Note:

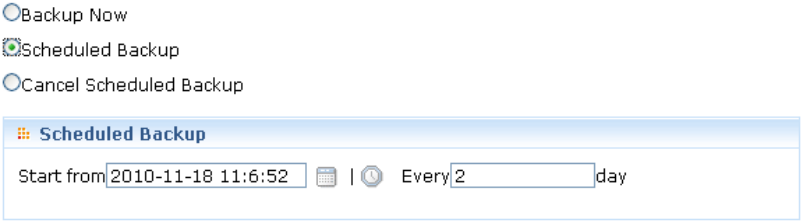
(1) If you haven't set the backup path, the operation of backup database can't be execute (The server for other computer to access, need to set the backup path in the server firstly).

(2) Proposal that the database backup path and the present system installed path not be under the same disk. Don't set the path to the root of a disk or the desktop.

2. Backup database:

Periodically backup the system's database to ensure data security. To use the backed up data, just restore the data.

(1) Click [Backup database] to enter the backup interface;



(2) Select from backup now, scheduled backup and cancel scheduled backup. Scheduled backup can set backup every several days since a start time;

(3) Click [OK]. For Backup now, it will return after backup. For scheduled backup, it will backup as scheduled.

Note:

(1) Please refresh the interface after database backup for a while to check the backup result. When the value of [Whether backup successful] turn from [Processing] to [Yes], the backup is complete, otherwise it turn to [No] and backup failure.

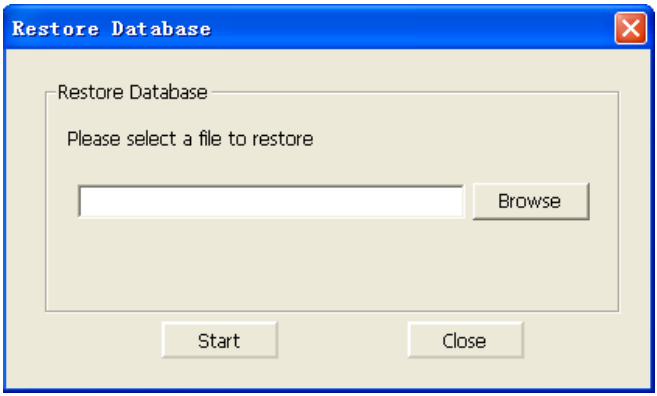
(2) We recommended to backup the database after you create the personnel file, device information or part of access control level settings.

(3) The system not support to backup Oracle database, if you need to backup, please use the specific Oracle backup tools.

3. Restore Database

Select [Restore Database] in the **[Server Controller]** operation menu, the following interface appear.

Click [Browse] to select a successfully backed up database from the backup database list, click [Start] begin the database restoration.



Note:

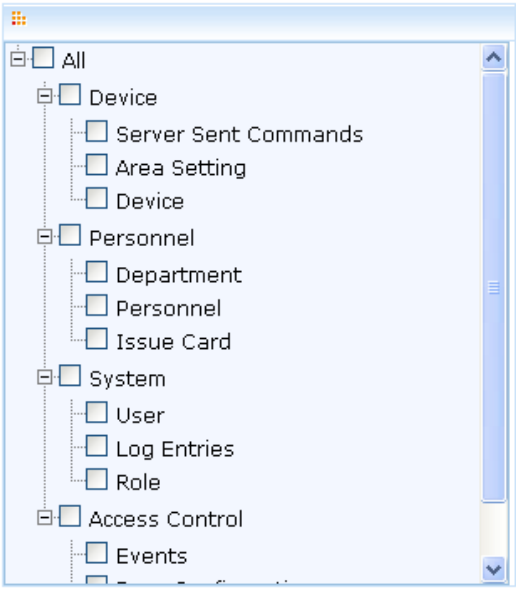
(1) Don't close any command window prompt during the database restore process.

(2) On the same server, please don't plan multiple scheduled backup to avoid adding to the server load.

4. Initialize database:

Initialize database is to restore data to system initialization status. Initialized data in the database will be deleted. Please operate with care.

Click [Initialize database] to enter edit interface, select one or several datasheets to initialize, and click [OK] to complete initialization and return.



For example:

Select to initialize access level: After selection, it will initialize access control time periods, access control holidays and access levels. All contents on these three pages will restore initial statuses;

Select to initialize door settings: After selection, it will initialize all interlock settings, anti-passback settings, linkage settings, first-card opening settings, and multi-card opening settings (including personnel group of multi-card verification);

Select to initialize events: After selection, it will initialize all real-time monitoring records;

Select to initialize access control: After selection, it will initialize all settings and information in the access control system, including the above three items, and only reserve system default settings;

Select to initialize devices: After selection, it will initialize all device information in the system (including access control). If the device is an access control panel, corresponding device parameters and door information will be deleted.

Note: If the device is still in normal use, please initialize database cautiously,

especially when involving access level-related departments and personnel, access levels, door settings, areas, devices, users and roles. It is recommended that if there are still devices in use after database initialization, the user shall [Synchronize all data] for the setting to avoid unexpected errors.

7.3 System parameters

The system homepage shows the system parameter list: Parameter name, Parameter value, Description, and Related operation.

7.4 Log records

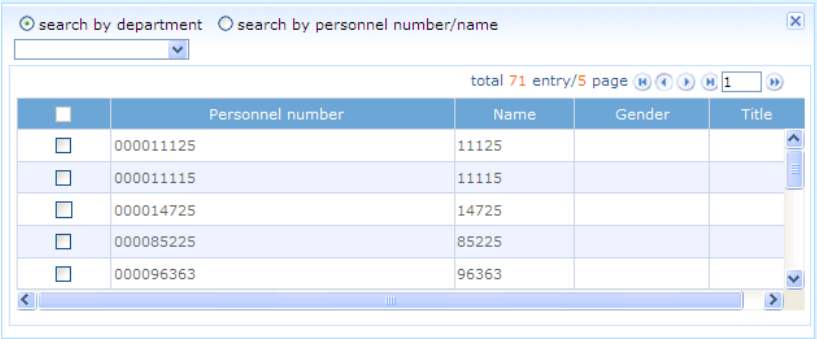
The default homepage of system log records shows log records of all operations. Since large data size, you can use query function to search desired log records. For details, see Appendix 1 Common Operation.

8. Appendices

Appendix 1 Common operation

1. Personnel selection

In this system, this dialog box is used for all modules using personnel selection:



You can search personnel in two ways:

1) Search by department. Tick the check box before a department in the department list of the pull-down menu to select all personnel of the department. If [Select all personnel under the department] is ticked, all personnel in the department will be selected and shown in the list box of the currently selected personnel;

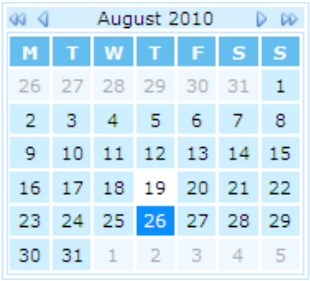
2) Search by personnel number/name. Enter the name or employee number of the person to be selected in the query box, and click query to show the eligible person in the list box.

When personnel are selected into the list box, if it is required to delete one or more persons, just cancel the tick of the check box before the personnel. To select or unselect all personnel in the list, click the 'Select all' check box under the list.

To cancel all personnel for reselection, click Clear.

2. Select date

Click the pull-down menu to select date:

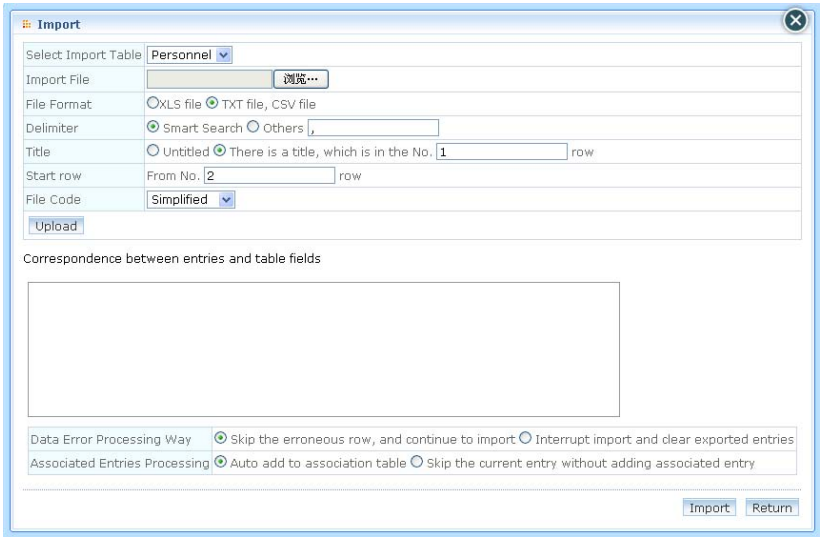


Click on year to activate the scroll button for year selection, and click or button to select an earlier or a later year. Click or button to select an earlier or a later month, and click the desired date.

3. Import (taking importing personnel table as an example):

If there is an electronic personnel file, which may be the information of the personnel or access control, attendance or human resources system of another brand, you can import it into this system through the [Import] function.

(1) Click [Import] to show the import edit interface:



Description of items:

Select import table: Currently the system supports the import of department table

and personnel table;

Import file: Click [Browse] to select the file to be imported;

File format: Select the format of the file to be imported;

Delimiter: The user select from smart search or others, such as comma, semicolon or blank;

Title: Select and set whether or not the original file contains a title. If so, enter which row the title is in;

Start row: The row from which importing starts (namely, which row of the original file the data in the first row is in);

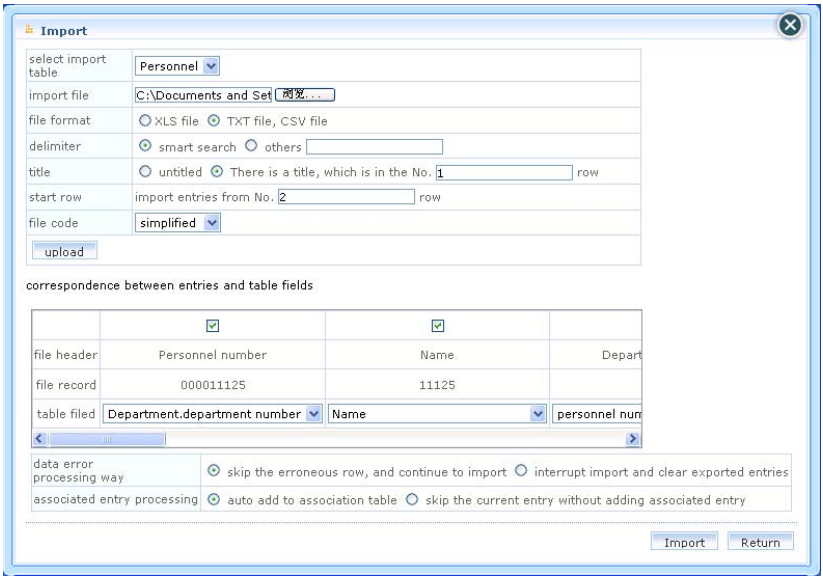
File code: Select the code that the original file uses, being Simplified Chinese or English;

Data error processing way: Select “skip the erroneous row, and continue to import”, or “interrupt import and clear imported entries”;

Associated entry processing: Select “auto add to associate table” or “skip the current entry without adding associated entry”.

(2) Click [Browse] to select the file to be imported;

(3) Click [Open] button, and the file format will be automatically shown. Determine delimiter, title, start row and file code, and click [Upload] to show the following window:



(4) In the table below [correspondence between entries and table fields], [file header] is an item row in the original file, [file record] is a data row in the original file, [table field] is an item in the current system. Select corresponding fields in the system from pull-down menus, and unwanted data can be unchecked.

(5) Select data error processing way and associated entry processing, click [Import], and the system will automatically start importing data. When the system prompts that data import is successful, the newly imported data will be shown in the personnel list.

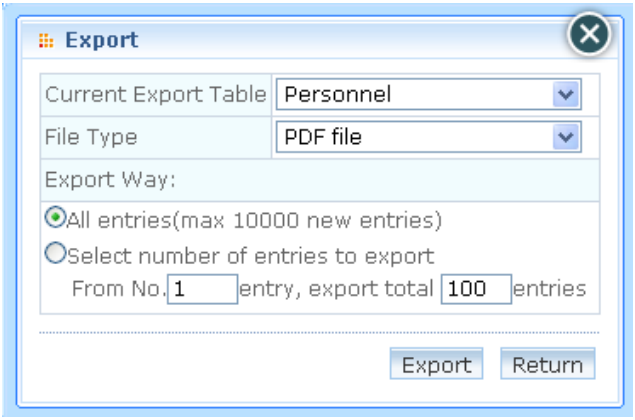
Note:

(1) When importing department table, repeated numbers do not affect import, and can be modified manually;

(2) When importing personnel table, if there is no personnel number or personnel number is "0", the import operation can't execute. If you need import the personnel gender, please use "M" represent male and "N" represent female, then execute import operation.

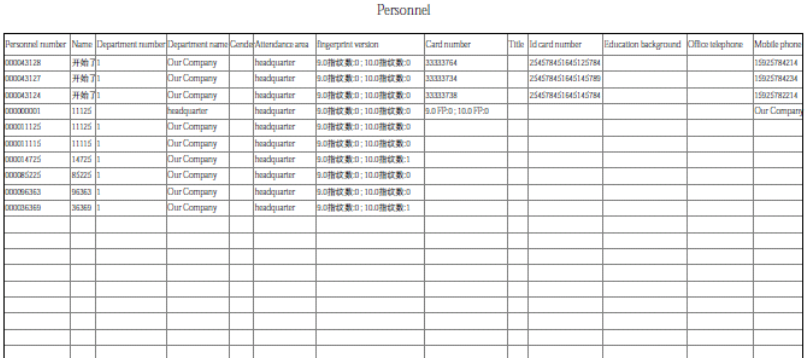
4. Export data (taking exporting personnel list as an example):

(1) Click [export] to show the edit interface:



When the data size is large, it is recommended to select [Select number of entries to export] to expedite export and reduce system load.

(2) Select the format of exported file: If PDF format is selected, there will be no file code option (namely, no differentiation between Simplified and Traditional Chinese). Click [Export] to directly show the exported file:



Personnel

Personnel number	Name	Department number	Department name	Gender	Attendance area	Fingerprint version	Card number	Title	Id card number	Education background	Office telephone	Mobile phone
000043128	开始了	1	Our Company		headquarter	9.0指纹数:0；10.0指纹数:0	33333764		254578451645125784			15925784214
000043127	开始了	1	Our Company		headquarter	9.0指纹数:0；10.0指纹数:0	33333734		254578451645145785			15925784234
000043124	开始了	1	Our Company		headquarter	9.0指纹数:0；10.0指纹数:0	33333738		254578451645145784			15925782214
000000001	11125		headquarter		headquarter	9.0指纹数:0；10.0指纹数:0	9.0 FP:0；10.0 FP:0					Our Company
00001125	11125	1	Our Company		headquarter	9.0指纹数:0；10.0指纹数:0						
00001115	11115	1	Our Company		headquarter	9.0指纹数:0；10.0指纹数:0						
00014725	14725	1	Our Company		headquarter	9.0指纹数:0；10.0指纹数:1						
00085225	85225	1	Our Company		headquarter	9.0指纹数:0；10.0指纹数:0						
00096363	96363	1	Our Company		headquarter	9.0指纹数:0；10.0指纹数:0						
00026369	36369	1	Our Company		headquarter	9.0指纹数:0；10.0指纹数:1						

If TXT or CSV format is selected, then file codes include Simplified and Traditional Chinese, but Traditional Chinese code can be completely exported only in the operating system in Traditional Chinese. The system prompts Open or Save:

Select [Open] to directly show the list. Select [Save] to pop up the [Save as] dialog box. Determine file name and save type, and select save path. Select [Cancel] to return.

(3) Return to the initial edit interface, and click [Return] to return to the personnel interface.

Note:

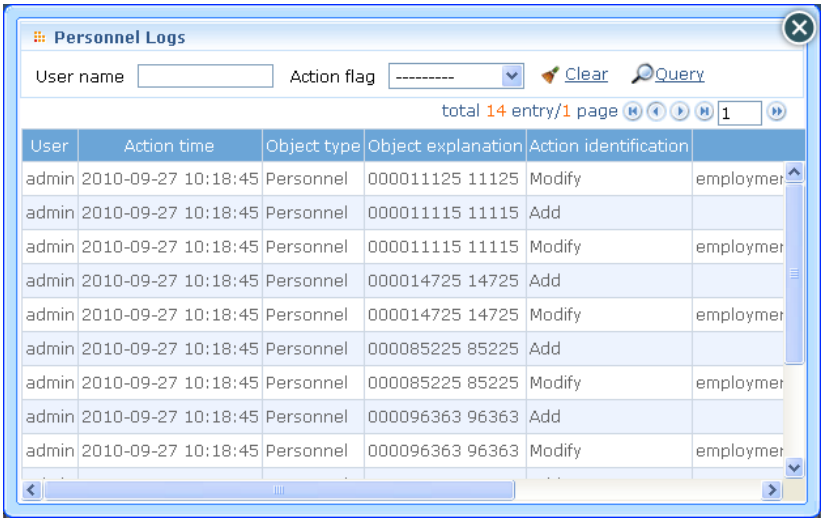
(1) When importing department table, repeated numbers do not affect import, and can be modified manually;

(2) Exported table is the list currently shown, being the list of queried or displayed result;

(3) Up to 10,000 latest records can be exported.

5. View log records (taking personnel log as an example):

(1) Click log records to show the following:



User	Action time	Object type	Object explanation	Action identification	
admin	2010-09-27 10:18:45	Personnel	000011125 11125	Modify	employmer
admin	2010-09-27 10:18:45	Personnel	000011115 11115	Add	
admin	2010-09-27 10:18:45	Personnel	000011115 11115	Modify	employmer
admin	2010-09-27 10:18:45	Personnel	000014725 14725	Add	
admin	2010-09-27 10:18:45	Personnel	000014725 14725	Modify	employmer
admin	2010-09-27 10:18:45	Personnel	000085225 85225	Add	
admin	2010-09-27 10:18:45	Personnel	000085225 85225	Modify	employmer
admin	2010-09-27 10:18:45	Personnel	000096363 96363	Add	
admin	2010-09-27 10:18:45	Personnel	000096363 96363	Modify	employmer

(2) Enter query condition, click [query] to show the list, click [Clear], clear query condition, and return to the initial interface.

Note:

1. The log records only show the operation log in the current operation module;

2. Log records under some operation menus can be viewed only when entering the edit interface.

For example, from [Access Control System] - [Door Configuration] - [Door Management], click [Edit] under "Related operation" of a device to enter the edit interface, and click [Log records] on the upper right corner of the interface to view the operation log.

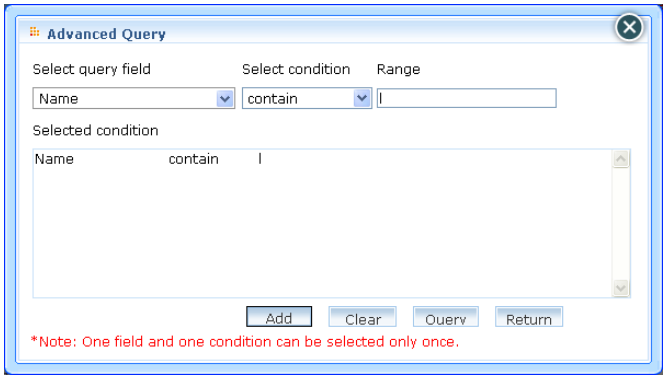
6. Query function (taking personnel information query as an example):

Common query: The user can directly select the item to be queried from [Common query] on my work panel, or enter a module for specific query.

Take personnel query as an example:

Enter query condition, click Query, and the query result will be shown below:

Advanced query: Click [Advanced] icon to show advanced query interface (taking personnel information advanced query as an example).



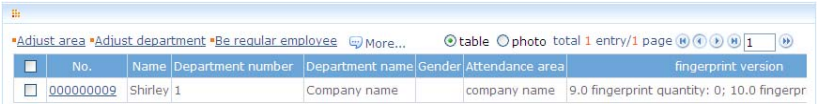
(1) Select the query field in the [Select query field] pull down menu;

(2) Select the condition in the pull down menu such as equal to null, contain, meet any, equal to etc.

(3) Input the query value in the [Range] field;

(4) Click [Add] to add this query information to the [Selected condition] list, the multiple choice of query condition is allowed. But one field and one condition can be selected only once.

Click [Query], the query result display on the list.



The query functions of each menu in the system are similar, differing in that query conditions are different, and the user can enter as prompted.

Appendix 2 END-USER LICENSE AGREEMENT FOR THIS SOFTWARE

Important - read carefully:

This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and the mentioned author of this Software for the software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE. This EULA grants you the following rights: Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.

Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Limitations on Reverse Engineering, De-compilation, and Disassembly. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable

law notwithstanding this limitation.

Separation of Components.

The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one computer.

Software Transfer.

You may permanently transfer all of your rights under this EULA, provided the recipient agrees to the terms of this EULA.

Termination.

Without prejudice to any other rights, the Author of this Software may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

Distribution.

The SOFTWARE PRODUCT may not be sold or be included in a product or package which intends to receive benefits through the inclusion of the SOFTWARE PRODUCT. The SOFTWARE PRODUCT may be included in any free or non-profit packages or products.

3. COPYRIGHT.

All title and copyrights in and to the SOFTWARE PRODUCT(including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by the Author of this Software. The SOFTWARE PRODUCT is protected by copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material except that you may install the SOFTWARE PRODUCT on a single computer provided you keep the original solely for backup or archival purposes.

LIMITED WARRANTY

NO WARRANTIES.

The Author of this Software expressly disclaims any warranty for the SOFTWARE PRODUCT. The SOFTWARE PRODUCT and any related documentation is provided "as is" without warranty of any kind, either express or implied, including, without limitation, the implied warranties or merchantability, fitness for a particular purpose, or non-infringement. The entire risk arising out of use or performance of the SOFTWARE PRODUCT remains with you.

NO LIABILITY FOR DAMAGES.

In no event shall the author of this Software be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if the Author of this Software has been advised of the possibility of such damages.

Acknowledgment of Agreement.

I have carefully read and understand this Agreement, Radiate, Inc.’s Privacy Policy Statement.

IF YOU ACCEPT the terms of this Agreement:

I acknowledge and understand that by ACCEPTING the terms of this Agreement.

IF YOU DO NOT ACCEPT the terms of this Agreement.

I acknowledge and understand that by refusing to accept these terms, I have rejected this license agreement and therefore have no legal right to install, use, or copy this Product or the Licensed Software that it incorporates.

Appendix 3 FAQs

Q: How can my work panel be unique?

A: The user can customize the work panel: 1. Click [Custom work panel] to pop up a dialog box, cancel the tick of your undesired module (by default the system ticks all), and Confirm. Then the custom module will appear; 2. Or directly click the " " icon on a module to minimize, and click " " to close the module. Click the column bar to drag and adjust the module's position; 3. If required to return to the default work panel, click [Restore work panel] to refresh and return to the system default.

Q: How to use a card issuer?

A: Connect the card issuer to PC through USB port, and then select individual personnel card issue or batch card issue. Move the cursor to the card number input box, and punch the card on the card issuer, then the card number will be automatically shown in the input box.

Q: What is the use of role setting?

A: Role setting has the following uses: 1. To set unified level for the same type of users newly added, just directly select this role when adding users; 2. When setting system reminder, determine which roles can be viewed.

Q: How to operate if I want to set accounts for all personnel of the Company's Financial Department?

A: First, create a new role in system setting and configure the functions to be used for this role. Then add a user, set user information, and select the user's role, thus adding a new account. For other accounts, do the same.

Q: What is the use of blacklist?

A: A blacklisted personnel can not achieve departure restoration, namely, this person can not be employed by the Company any longer. To modify, just modify departure information on the departure interface.

Q: How to adjust the department of a person?

A: There are the following ways to adjust personnel department: 1. In personnel list, click personnel number or click "Edit" under related operation item to show personnel details, and modify personnel department in the department item; 2. In personnel list, check the personnel requiring department adjustment, click "Adjust department", and a dialog box will pop up, then modify the department; 3. On personnel transfer interface, click Add to pop up the edit interface, select personnel, and check department in the transfer field, and complete other information, thus

completing transfer.

Q: How to set access levels for visitors?

A: Setting access levels is as follows: 1. In the system, add these personnel, and enter relevant information; 2. Select access levels suitable for them. If there are no suitable levels, it is required to enter the access control system to add relevant settings; 3. Set valid time, namely, the start and end dates when they need to use access levels.

Q: What are the ways to cancel personnel access control settings?

A: There are the following ways to cancel personnel access control settings: 1. Close access control only: In the personnel list, click personnel number or click "Edit" under related operation item to show personnel details, and delete access levels and Personnel Group of Multi-Card Verification in access control settings; 2. Delete personnel: In the personnel list, click "Delete" under related operation item of personnel, or tick a personnel and click the "Delete" above to delete this person from the system. Corresponding access control information will be deleted; 3. In "Personnel access levels settings", delete access levels of personnel, and in "Personnel Group of Multi-Card Verification", delete Multi-Card Opening levels.

Q: How to set access control holidays?

A: Access control holidays have three types of 1, 2 and 3. Take New Year's Day as an example: 1. In access control holidays, add a holiday of "New Year's Day". Set the holiday type as 1, and the start and end dates of the holiday are both January 1; 2. During the access control time period, add an access control time zone, set the three access control intervals of this holiday type 1. For example, set access control interval 1 as 8:00-20:00, and intervals 2 and 3 as null, namely Normal Close; 3. Apply this access control time zone to access levels; 4. Set personnel with levels for the access levels.

Q: In Windows Server 2003, why the IE browser displayed error when access the system, how to solve it?

A: This problem occurs because that Server 2003 has a [Security Configuration Option] settings. If you want access the system, please configure it as follows: click Start – Control Panel – Add or Remove Program, select [Add and remove Windows components] in the interface and click [Internet Explorer Enhanced Security Configuration] option, cancel the tick before it. Then click [Next] to remove it from the system. Open the system again, the browser will access the system properly.

Q: If backuping or restoring the database fails, the possible reason?
A: Please check the system environment variables [path], if the database installation path (For example, MS SQL Server installation path maybe is: C:\Program Files\Microsoft SQL Server\90\Tools\Binn; For MySQL, it is like: C:\Program

Files\MySQL\MySQL Server 5.1\bin) is exist. If not, you need to add it manually. Otherwise, the antivirus or firewall software may stop the execution of backuping or restoring command, if the security prompt pops up, please select “Always Permitted”.And the damaged database can also lead to backup error, please repair or restore the database.